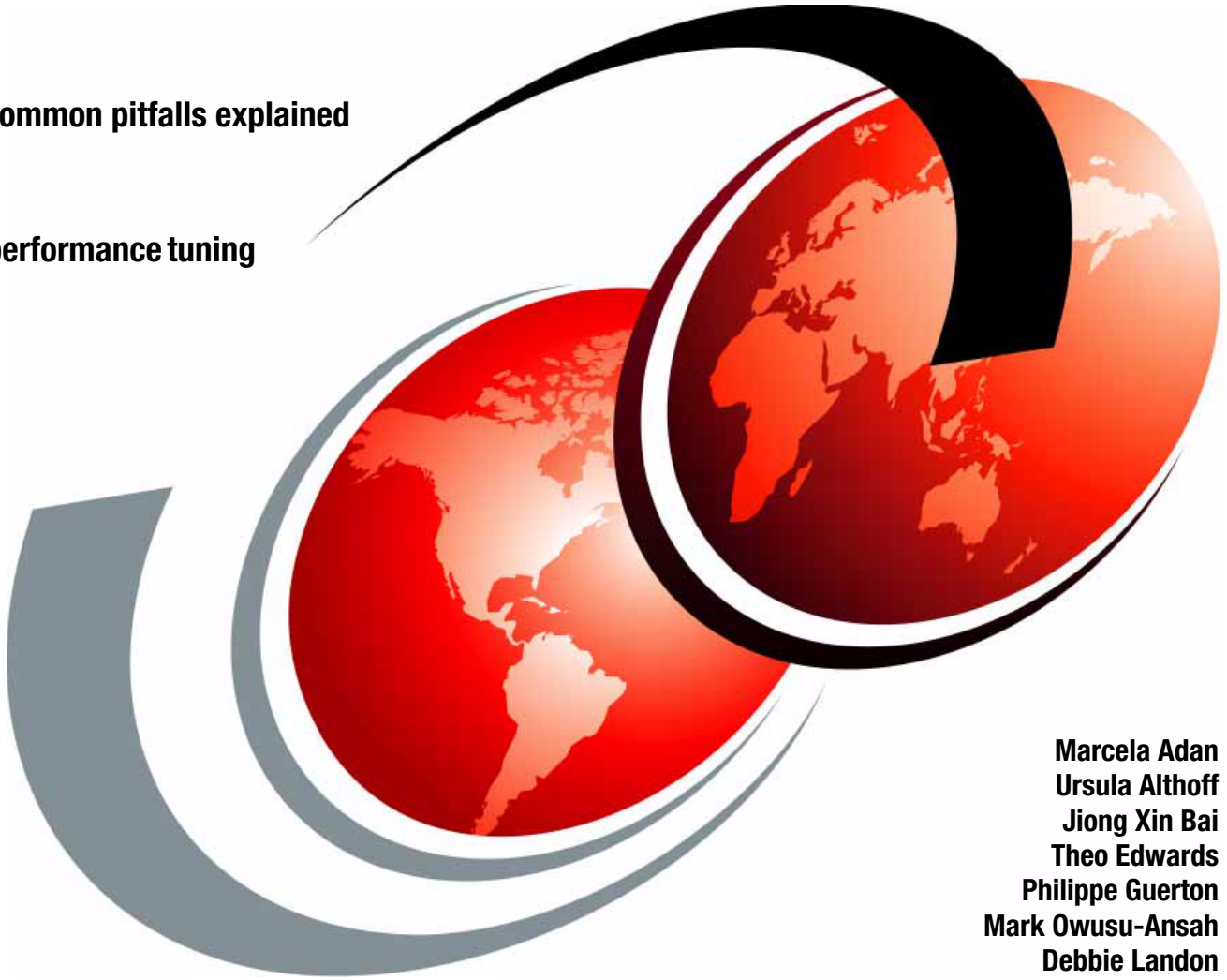
WebSphere. software

IBM

Installing and Configuring WebSphere Portal Express V6 on i5/OS

- Comprehensive step-by-step guide
- Tips and common pitfalls explained
- Practical performance tuning guidelines



Marcela Adan
Ursula Althoff
Jiong Xin Bai
Theo Edwards
Philippe Guerton
Mark Owusu-Ansah
Debbie Landon

Redpaper

ibm.com/redbooks

International Technical Support Organization

Installing and Configuring WebSphere Portal Express V6 on i5/OS

November 2007

REDP-4303-00

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (November 2007)

This edition applies to IBM WebSphere Portal Express V6 running i5/OS V5R3 or later.

© Copyright International Business Machines Corporation 2007. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices vii
Trademarks viii

Preface ix
The team that wrote this paper ix
Become a published author xi
Comments welcome xi

Chapter 1. Introduction to WebSphere Portal Express V6 on i5/OS 1
1.1 WebSphere Portal Express V6.0 overview 2
1.2 Positioning in the WebSphere Portal family 3
1.3 WebSphere Portal Express packaging on i5/OS 6
1.4 Why use i5/OS as a platform for WebSphere Portal Express 7
1.4.1 Consolidation of different workloads in a single server 7
1.4.2 Vertical scalability 9
1.4.3 i5/OS exclusive functions for WebSphere Portal Express 9
1.4.4 iSeries Access for Web portlets and single sign-on 10
1.4.5 Running multiple portal profiles and versions in a single system 11
1.4.6 i5/OS integration and low total cost of ownership 12
1.4.7 Benefits for existing System i clients 13
1.5 System i models for WebSphere Portal Express 14

Chapter 2. Preparing your i5/OS environment for WebSphere Portal Express 15
2.1 Sizing the system 16
2.2 Downloading the WebSphere Portal Express images 16
2.3 Assembling the WebSphere Portal Express images 20
2.3.1 Assembling the WebSphere Application Server product 20
2.3.2 Assembling WebSphere Portal Express 20
2.4 i5/OS configuration and network requirements 21
2.4.1 Verifying the i5/OS time zone 21
2.4.2 Verifying the Coded Character Set Identifier 22
2.4.3 Verifying language settings of system values and user profiles 22
2.4.4 Network requirements 24
2.5 i5/OS software requirements 29
2.5.1 Displaying installed i5/OS software 30
2.6 Program temporary fixes 32
2.6.1 Required i5/OS V5R3 PTFs 33
2.6.2 Required i5/OS V5R4 PTFs 33
2.6.3 Verifying group PTFs 34
2.7 Installing WebSphere Application Server 36
2.7.1 Installing the WebSphere Application Server PTF group 36
2.7.2 Verifying the WebSphere Application Server environment 37
2.7.3 Installing interim fix after installing WebSphere Application Server fix pack 19 . . 39
2.8 Preparing the IBM Directory Server for i5/OS 39
2.8.1 Supported LDAP directories 40
2.8.2 Terminology 40
2.8.3 Using the default LDAP suffix 41
2.8.4 Creating a new LDAP suffix 43

© Copyright IBM Corp. 2007. All rights reserved.

2.9 Supported Web browsers 46

Chapter 3. Installing and configuring WebSphere Portal Express 47
3.1 Installing WebSphere Portal Express from electronic images. 48
3.1.1 Install only option (recommended method) 48
3.1.2 Install and configure option 59
3.1.3 Common installation problems 67
3.1.4 Verifying the WebSphere Portal Express installation 69
3.2 Configuring WebSphere Portal Express with IBM Web Administration for i5/OS 71
3.2.1 Verifying the HTTP Administration server is active 71
3.2.2 Configuring the WebSphere Portal profile. 73
3.2.3 Accessing logs via IBM Web Administration for i5/OS 87
3.3 Understanding WebSphere Portal Express work management on i5/OS. 90
3.3.1 WebSphere Portal Express product components on i5/OS 90
3.3.2 Identifying application servers associated with a portal profile 93
3.3.3 Starting and stopping portal servers 94
3.3.4 Starting portal servers when QWAS6 subsystem starts 96
3.4 Problem determination 96
3.4.1 Installation log files 97
3.4.2 Configuration log files 98
3.4.3 WebSphere Portal Express version and history information. 98
3.5 Deleting a WebSphere Portal Express profile. 101
3.6 Uninstalling the WebSphere Portal Express product 103

Chapter 4. Initial performance tuning 105
4.1 Web Performance Advisor 106
4.1.1 Prerequisites 106
4.1.2 Accessing the Web Performance Advisor. 106
4.1.3 System attributes 109
4.1.4 Web Environment attributes 110
4.1.5 Adjusting parameters 113
4.1.6 Additional tuning parameters 114
4.2 System tuning 115
4.2.1 Processor multitasking: QPRCMLTTSK 115
4.2.2 Maximum activity level of system: QMAXACTLVL 116
4.2.3 Performance adjustment: QPFRADJ 116
4.2.4 Machine storage pool size: QMCHPOOL 117
4.2.5 Parallel processing degree: QQRYDEGREE 118
4.2.6 Thread resource adjustment: QTHDRSCADJ. 119
4.2.7 Thread resource affinity: QTHDRSCAFN 119
4.3 Memory tuning 120
4.3.1 Running WebSphere Portal in a dedicated memory pool 121
4.3.2 Memory pool size 122
4.3.3 Memory pool activity level. 123
4.3.4 Memory pool expert cache 124
4.4 Disk tuning 125
4.5 Machine setup. 126
4.5.1 Processors 126
4.5.2 Direct Access Storage Devices. 126
4.5.3 PTFs 127
4.6 TCP/IP. 128
4.6.1 Line speed and duplex support. 128
4.6.2 Maximum frame size. 128

4.6.3 Maximum transmission unit. 128
4.6.4 Send and receive buffer sizes. 130
4.7 HTTP Server 130
4.7.1 Traffic compression. 130
4.7.2 General server configuration. 131
4.7.3 HTTP connections 133
4.7.4 Logging levels 134
4.8 WebSphere Application Server 137
4.8.1 Default application server 137
4.8.2 Java Virtual Machine. 137
4.8.3 Caching. 142
4.8.4 Servlet engine thread pool 144
4.8.5 Session timeout 147
4.8.6 Logging level. 148
4.9 Database. 150

Chapter 5. Enabling Secure Sockets Layer 153
5.1 SSL between WebSphere Portal Express and the LDAP server 155
5.1.1 Certificate management 155
5.1.2 Enabling SSL for the LDAP server 170
5.1.3 Enabling SSL for WebSphere Portal Express. 181
5.2 SSL between WebSphere Portal Express and Web browser 183
5.2.1 Enabling the HTTP server for SSL 183
5.2.2 Enabling WebSphere Application Server for SSL. 198
5.2.3 Enabling WebSphere Portal Express for SSL: login only 217
5.2.4 Enabling WebSphere Portal Express for SSL: All pages 227

Chapter 6. Online backup and recovery 241
6.1 Backup and recovery process. 242
6.2 Offline backup and restore using scripts 244
6.2.1 Example of an offline backup 244
6.2.2 Example of restore using scripts. 245
6.3 Online backup using BRMS 245
6.3.1 Creating a backup policy using the Backup Policy wizard 247
6.3.2 Scheduling your backup with the advanced job scheduler 287
6.3.3 Running an online backup of the WebSphere Portal Express V6 server 288
6.4 Scenario 1: Restoring in one step from data saved with a backup policy 291
6.4.1 Running the PreExpressRestore.sh script 292
6.4.2 Restoring all saved components in one step 294
6.4.3 Running the PostExpressRestore.sh script. 304
6.5 Scenario 2: Restoring individually from data saved with a backup policy 306
6.5.1 Running the PreExpressRestore.sh script 306
6.5.2 Restoring all schemas and database libraries 306
6.5.3 Restoring the HTTP server member object. 317
6.5.4 Restoring user profile and security data 319
6.5.5 Restoring the integrated file system files 320
6.5.6 Running the PostExpressRestore.sh script. 327
6.6 Using the BRMS commands for backup and restore 327
6.6.1 Running a backup with a policy using i5/OS commands 328
6.6.2 Restoring with a policy using i5/OS commands 333

Appendix A. Upgrading to WebSphere Portal Express V6.0.1 347
Preparing for the upgrade 348
Upgrading to WebSphere Portal Express V6.0.1 351
Post-installation steps 352

Appendix B. Additional material 359
Locating the Web material 359
Using the Web material 359

Related publications 361
IBM Redbooks publications 361
Other publications 361
Online resources 361
How to get IBM Redbooks publications 362
Help from IBM 362

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

© Copyright IBM Corp. 2007. All rights reserved.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ®
developerWorks®
eServer™
iSeries®
i5/OS®
AIX®
AS/400®
Domino®
DB2 Universal Database™
DB2®
IBM®
Lotus®
NetServer™
Operating System/400®
OS/400®
PartnerWorld®
Passport Advantage®
Perform™
POWER5™
QuickPlace®
Redbooks®
Sametime®
System i™
System i5™
Tivoli®
WebSphere®
Workplace™
Workplace Forms™
Workplace Web Content Management™

The following terms are trademarks of other companies:

SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Java, JDBC, JSP, JVM, J2EE, Sun, Sun Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Active Directory, Internet Explorer, Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redpaper provides an overview of the WebSphere Portal V6.0 family on the System i platform and positions WebSphere Portal Express V6.0 within the portal family. This IBM Redpaper provides information about how to prepare your System i i5/OS® environment before you install and configure WebSphere Portal Express V6. It includes step-by-step instructions that help system administrators and IT consultants to quickly deploy WebSphere® Portal Express into a production environment on a System i machine.

This Redpaper also includes information that helps you perform the initial tuning of your portal environment. It explains how to configure Secure Sockets Layer (SSL) to protect sensitive login information to the portal and LDAP servers. Finally, it explains how to save a WebSphere Portal Express V6 profile while it is online and actively in use.

The team that wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Rochester Center.

Marcela Adan is a Consultant IT Specialist in the System i™ Technology Center (iTC) in Rochester, Minnesota. She leads the team responsible for accelerating the adoption of new WebSphere and Collaboration technologies on the IBM System i platform. She is responsible for designing, planning, and implementing early enablement, education, and support programs aimed at facilitating the adoption of WebSphere, portal, and collaboration solutions on the System i platform. Marcela has held several positions in development, consulting, technical support, and skills transfer. She is a frequent speaker at technical conferences and teaches IBM classes worldwide. You can contact Marcela by sending e-mail to adan@us.ibm.com.

Ursula Althoff is working at STG Sales as an IT Specialist for System i Technical Sales in Germany. She has worked at IBM for 31 years. Her experience in midrange computers started with S/38 and AS/400®. Her areas of experience include i5/OS, application development, WebSphere Application Server on i5/OS, and WebSphere Development Client for iSeries®. She has developed courses about e-business on System i for IBM Learning Services, written articles, and also co-authored several IBM Redbooks® about these topics. You can contact Ursula by sending e-mail to usalthoff@de.ibm.com.

© Copyright IBM Corp. 2007. All rights reserved.

Jiong Xin Bai is a Senior Product Support Professional in IBM China. She joined IBM in 1999 and worked in the Lotus® support organization since then. In 2006, Jiong Xin joined the WPLC World Wide Support Engineering Team, which is focused on technical support for critical situations. Her expertise is in Lotus Domino® and other Domino-based products and solving complex, cross-platform, and cross-product problems. You can contact Jiong Xin by sending e-mail to baijx@cn.ibm.com.

Theo Edwards is a Staff Software Engineer with the IBM Software Group in the United States. He specializes in support and solution deployment strategy around WPLC Products for System i framework. He has advanced and in-depth professional knowledge of IBM Software Development, system, and product design. His current focus is on WebSphere Portal Architectural Design and Integration concept. Before joining IBM in 1999, Theo worked as a System Specialist and Application Programmer for a number of industries hosting e-business on System i. Theo has contributed to numerous technical solution papers regarding Domino, Workplace™ and WebSphere Portal. His publications are available on the IBM Software Knowledge Base Web site. He is also a member of COMMON, an IBM users group. You can contact Theo by sending e-mail to theo_edwards@us.ibm.com.

Philippe Guerton is an IT Specialist from the European Business Solutions Center at La Gaude, France. As a member of the IBM System and Technology Group Lab Services Europe, he provides service for leading edge IBM technologies for the IBM eServers, mainly System i5™, including WebSphere Portal, high availability, and back-end integration (SAP®, JDE, 5250 applications, and so on). For the past three years, he has focused on J2EE™, concentrating mainly on the Web enablement of native iSeries applications using HATS, WebFacing, WDHT, and IBM Toolbox for Java™. Before joining IBM STG Lab Services, he was part of IBM Global Services providing on-site expertise for ILE developments, and for SAP implementations as an SAP Basic Components consultant. You can contact Philippe by sending e-mail to p_guerton@us.ibm.com.

Mark Owusu-Ansah is an Advisory Software Engineer who works at the Domino Support center in West Chester, PA. He is a certified iSeries Domino Technical Solutions V5R3 Specialist and has extensive experience supporting Domino and associated products on i5/OS. His current focus is supporting Workplace™ Services Express and portal implementations on i5/OS. He holds various other certifications, including Certified Java Programmer, IBM Certified Advanced Application Developer - Domino 6/6.5, and Principal CLP R5/Domino 6. He also attained IBM Certified Advanced Technical Expert - AIX® status when he supported Domino products on UNIX® systems before joining the Domino on i5/OS support team. He has been with IBM for seven years. You can contact Mark by sending e-mail to mark_owusu-ansah@us.ibm.com.

Debbie Landon is an IBM Certified Senior IT Specialist in the IBM ITSO, Rochester Center. Her current area of expertise is the System i collaboration products, including IBM Lotus Domino and related Lotus products, such as Sametime® and QuickPlace®. Debbie has been with IBM for 24 years working first with the S/36 and then the AS/400, which has since evolved to the iSeries server and is now the IBM System i platform. Before joining the ITSO in November of 2000, Debbie was a member of the PartnerWorld® for Developers iSeries team, supporting IBM Business Partners in the area of Domino for iSeries. You can contact Debbie by sending e-mail to dalandon@us.ibm.com.

Thanks to the following people for their contributions to this project:

Erik Bjorklund
Jon Brandt
Jody Mueller
Tim Rowe
IBM Rochester Development Lab

CD Choi
IBM Raleigh Development Lab

Thomas Gray
Joanna Pohl-Misczyk
Craig Schmitz
Jenifer Servais
International Technical Support Organization, Rochester Center

Dorothy Wu
developerWorks®, San Jose

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, IBM Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review IBM Redbooks publications form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

Introduction to WebSphere Portal Express V6 on i5/OS

This chapter provides an overview of the WebSphere Portal V6.0 family on the System i platform and positions WebSphere Portal Express V6.0 within the portal family. It includes a brief summary of the benefits of System i as a deployment platform for WebSphere Portal Express. This chapter discusses the following topics:

- "WebSphere Portal Express V6.0 overview" on page 2
- "Positioning in the WebSphere Portal family" on page 3
- "WebSphere Portal Express packaging on i5/OS" on page 6
- "Why use i5/OS as a platform for WebSphere Portal Express" on page 7
- "System i models for WebSphere Portal Express" on page 14

© Copyright IBM Corp. 2007. All rights reserved.

1.1 WebSphere Portal Express V6.0 overview

WebSphere Portal Express is the newest member of the WebSphere Portal V6.0 family. There are many enhancements and new functions included in WebSphere Portal V6. WebSphere Portal Express is based on the latest version of WebSphere Portal, and it shares the same core code and basic functions. Some of the features of WebSphere Portal Express V6 are:

- Install and configure as shipped intranet and extranet example sites to easily tailor a client's specific needs.
- Authorized users and administrators can customize the user's experience. The portal interface includes new themes, drag and drop customization, and fly-out menus.
- A site using personalization might show different news articles to managers than to regular employees, or different information to clients based on client type and sales campaigns.
- Web content management reduces implementation time and costs by placing content creation and management in the hands of content experts for "author once, publish everywhere" control. The result is more accurate and frequently updated Web content.
- Document management tools enable users to easily share, view, and organize files of all types in a central location.
- Support for access to a wide variety of applications, including Lotus Domino, Microsoft® Office, and Microsoft Windows® applications. These applications help users work with the applications they already know in the portal environment.
- Instant messaging to provide users with the ability to contact each other in the context of the work they are doing.
- Lotus Component Designer is an innovative, easy-to-use, and standards-based development tool that allows application designers to easily create components for WebSphere Portal Express.
- WebSphere Portlet Factory and Workplace Dashboard Framework provide extended capabilities.

WebSphere Portal Express V6 shares the same core code with the enterprise versions of WebSphere Portal V6. IBM portal technology, which is the market leader, is now available to small and medium businesses. WebSphere Portal Express provides flexible pricing and licensing options enabling organizations to start with as few as 20 users, and then expand as their business grows. Because they share the same code, the transition to the enterprise versions of WebSphere Portal is seamless.

Clients can have these benefits from WebSphere Portal Express V6:

- Create stronger client relationships, improve customer service, retention, and satisfaction by creating a personalized customer portal with accurate and up-to-date information and easy access to existing System i back-end applications and data.
- Leverage existing investments. WebSphere Portal Express provides easy access to existing mail and calendaring systems, whether they are Lotus Domino, Microsoft Exchange, POP3, or IMAP servers. System i clients can extend their investment in Domino applications and QuickPlace by accessing them using the portlets provided with WebSphere Portal Express or available via the WebSphere Portal catalog.

  5250 applications that have been modernized using Web facing technologies, such as WebFacing Deployment Tool with HATS Technology (WDHT), can be accessed through a portal. iSeries Access for Web portlets offer Web browser-based access to System i machines. iSeries Access for Web portlets enable users to leverage business information,

applications, and resources across an enterprise by extending the System i resources to the client desktop through a Web browser. Clients can assemble components into composite applications that are projected to users through a compelling front-end portal. Clients can reuse existing applications in a portal environment more easily than the original application. Organization data kept in multiple applications and data stores is consolidated in a single view.

- Be more responsive. Provide employees, clients, and partners with access to Web sites where the needed information and applications have been consolidated, organized, and personalized for easy access and use.
- Improve employee productivity and collaboration. WebSphere Portal Express improves access to the corporate directory with the people finder portlet. People awareness and Sametime facilitate access to people within the portal environment. WebSphere Portal Document Manager provides a central document repository for team collaboration. Employees can share documents while providing security features to grant the proper access to authorized people. Document management includes lock-in, versioning, and workflow approval capabilities. People awareness displays the name and status (online or offline) of the author of the document and the modifier, the person who has the document locked, and the name of the task owner in the workflow. Users can send links to documents and folders via e-mail instead of sending large attachments.
- Improve the accuracy and quality of the information. The Web Content Management technology included with WebSphere Portal Express makes it easier for subject matter experts to develop and update content quickly.
- Additional benefits for System i clients are:
  - i5/OS WebSphere Portal Express Web configuration wizard makes it easier to get faster time to value. WebSphere Portal Express V6 includes backup and recovery scripts for IBM i5/OS.
  - WebSphere Portal, HTTP server, LDAP server, database, Sametime, Domino, QuickPlace, and i5/OS applications can all run on a single system or multiple logical partitions (LPARs) in a single System i machine.
  - If your business needs grow, your portal infrastructure can grow on a single System i machine by sustaining an increased number of users and transactions and adding processor and memory resources.
  - Significant security and reliability characteristics of the System i platform are a big plus for portal deployments.

1.2 Positioning in the WebSphere Portal family

Figure 1-1 on page 5 shows the WebSphere Portal V6 offerings available on i5/OS. Functions included in each WebSphere Portal V6 offering are:

- Common WebSphere Portal services available on all offerings are:
  - Presentation
  - Customization
  - Application aggregation
  - Portlet application programming interface (API)
  - Use of hundreds of portlets
  - Web services for remote portlets (WSRP) support
  - WebSphere Portlet Factory runtime
  - Administration
  - Single sign-on

  - Search
  - Personalization
  - Virtual portlets
  - Multiple lightweight directory access protocol (LDAP) support
- Additional functions included in WebSphere Portal Express are:
  - Web Content Management
  - WebSphere Portal Document Management
  - Instant Messaging (Sametime 7.5)
  - Lotus Component Designer
- Additional functions included in WebSphere Portal Server are:
  - Cluster support
  - WebSphere Portlet Factory Designer (only for processor-based licensing)
- Additional functions included in WebSphere Portal Enable are:
  - Cluster support
  - Web Content Management
  - WebSphere Portal Document Management
  - WebSphere Portlet Factory Designer
  - Workflow Engine (not supported on i5/OS)
- Additional functions included in WebSphere Portal Extend are:
  - Cluster support
  - Web Content Management
  - WebSphere Portal Document Management
  - WebSphere Portlet Factory Designer
  - Sametime 7.0
  - Quickplace 7.0
  - Domino 7.0.1
  - Workflow Engine (not supported on i5/OS)
  - Workflow Builder (not supported on i5/OS)
  - Electronic Forms (supported on Windows)
  - Workplace Forms™ Server, Designer, and Viewer (supported on Windows)

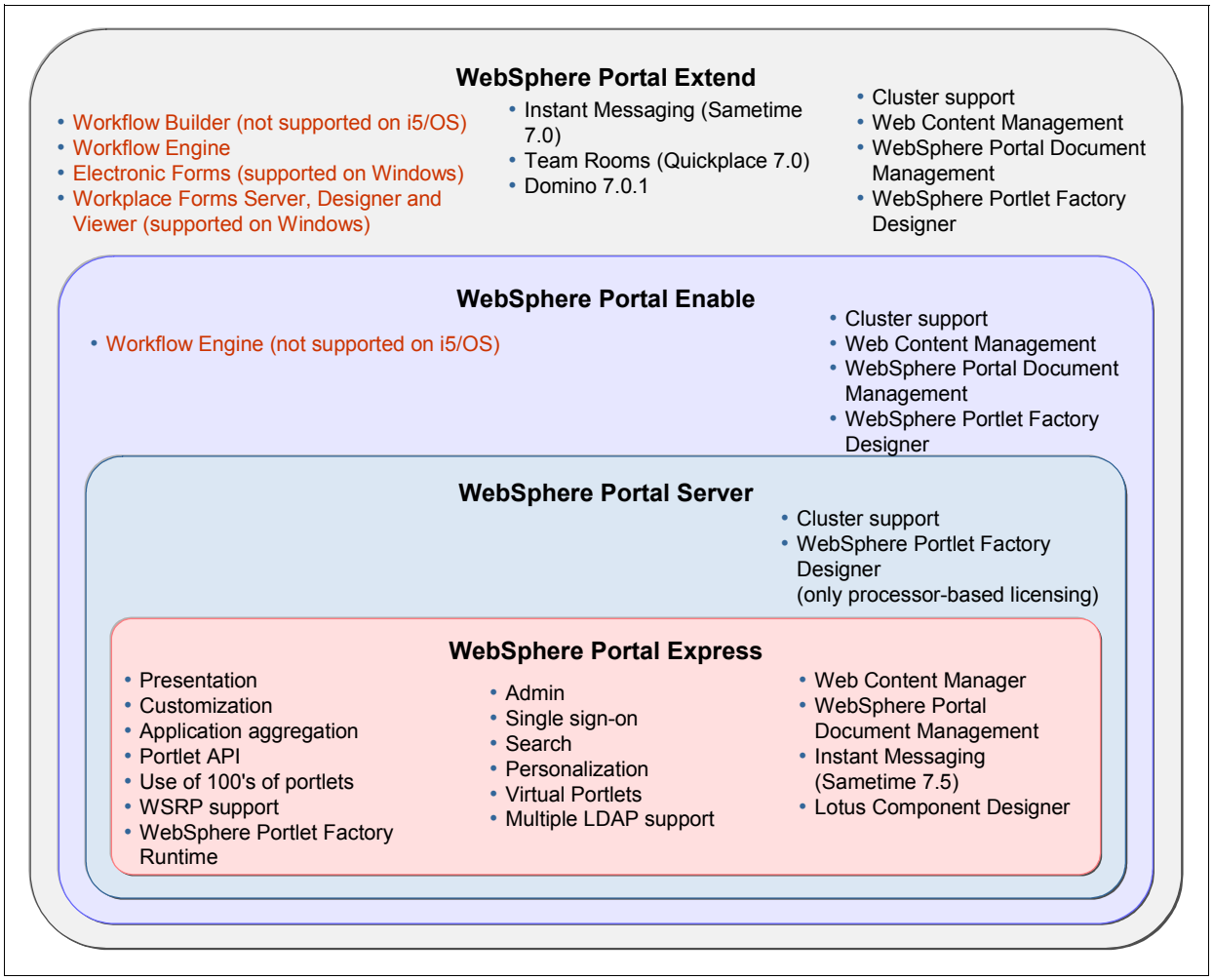

WebSphere Portal Extend
• Workflow Builder (not supported on i5/OS)
• Workflow Engine
• Electronic Forms (supported on Windows)
• Workplace Forms Server, Designer and Viewer (supported on Windows)
• Instant Messaging (Sametime 7.0)
• Team Rooms (Quickplace 7.0)
• Domino 7.0.1
• Cluster support
• Web Content Management
• WebSphere Portal Document Management
• WebSphere Portlet Factory Designer
WebSphere Portal Enable
• Workflow Engine (not supported on i5/OS)
• Cluster support
• Web Content Management
• WebSphere Portal Document Management
• WebSphere Portlet Factory Designer
WebSphere Portal Server
• Cluster support
• WebSphere Portlet Factory Designer (only processor-based licensing)
WebSphere Portal Express
• Presentation
• Customization
• Application aggregation
• Portlet API
• Use of 100's of portlets
• WSRP support
• WebSphere Portlet Factory Runtime
• Admin
• Single sign-on
• Search
• Personalization
• Virtual Portlets
• Multiple LDAP support
• Web Content Manager
• WebSphere Portal Document Management
• Instant Messaging (Sametime 7.5)
• Lotus Component Designer

Figure 1-1 WebSphere Portal offerings on i5/0S

Figure 1-2 on page 6 shows the WebSphere Portal V6.0 family and the positioning of WebSphere Portal Express in the family. WebSphere Portal Express is a single server solution (clustering is not supported). It has similar functionality to WebSphere Portal Enable (except for workflow engine and cluster support), and it adds the bundle of Sametime 7.5 for instant messaging and presence awareness. Other collaboration applications, such as Domino, QuickPlace, and Microsoft Exchange, can be integrated with WebSphere Portal Express via available portlets.

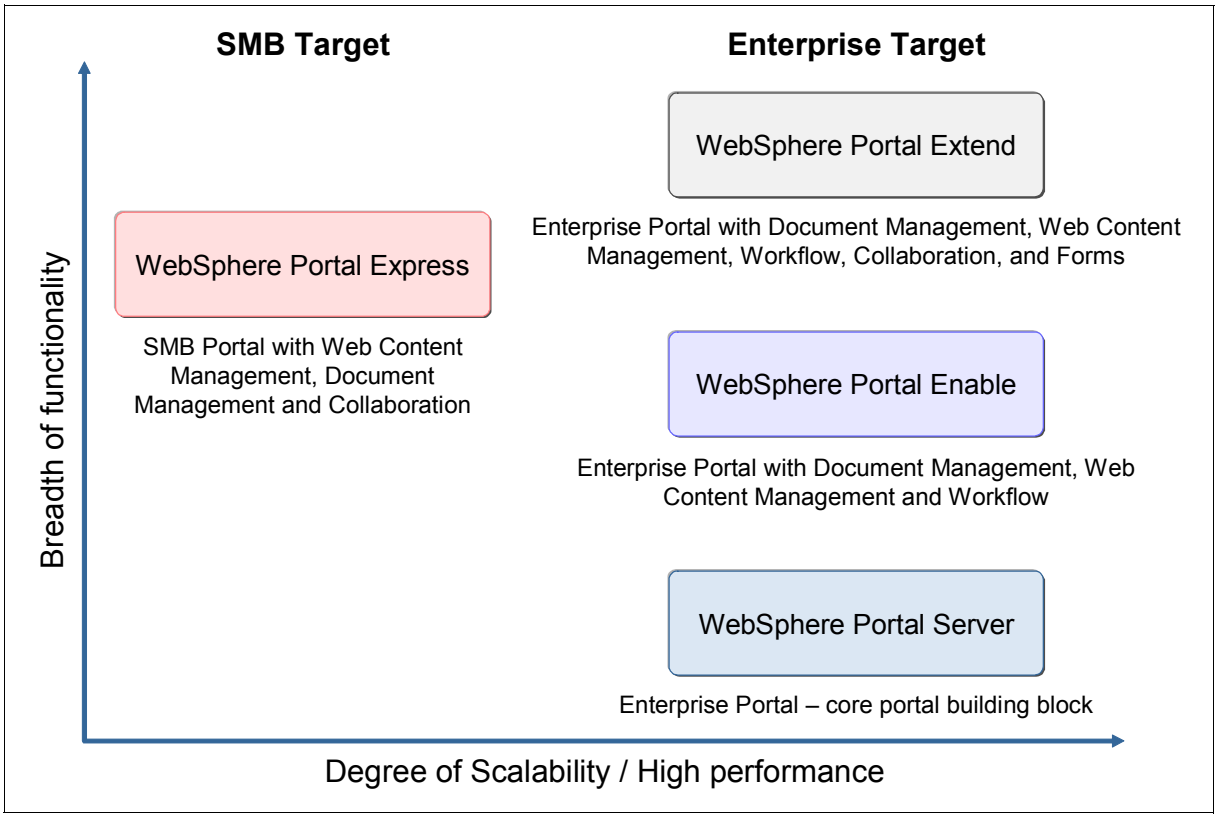

SMB Target
Enterprise Target
WebSphere Portal Extend
Enterprise Portal with Document Management, Web Content Management, Workflow, Collaboration, and Forms
WebSphere Portal Express
SMB Portal with Web Content Management, Document Management and Collaboration
WebSphere Portal Enable
Enterprise Portal with Document Management, Web Content Management and Workflow
WebSphere Portal Server
Enterprise Portal – core portal building block
Breadth of functionality
Degree of Scalability / High performance

Figure 1-2 WebSphere Portal Express positioning within WebSphere Portal V6.0 family

For more information about the WebSphere Portal family, see *Web Portal software from WebSphere* at:

`http://ibm.com/websphere/portal`

1.3 WebSphere Portal Express packaging on i5/OS

Figure 1-3 on page 7 shows the WebSphere Portal Express for i5/OS packaging.

The components in blue marked with one asterisk (*) are included with the base i5/OS operating system. They are:

- i5/OS V5R3 or V5R4 (and prerequisite licensed products listed in 2.5, “i5/OS software requirements” on page 29)
- DB2® for i5/OS
- IBM HTTP server
- IBM Directory Server (LDAP)
- WebSphere Portal Web configuration wizard included in IBM Web Administration for i5/OS

The other components in the WebSphere Portal Express package run on i5/OS, or on Windows as indicated in Figure 1-3 on page 7. Notice that the WebSphere Application Server prerequisite products are included in the WebSphere Portal Express package.

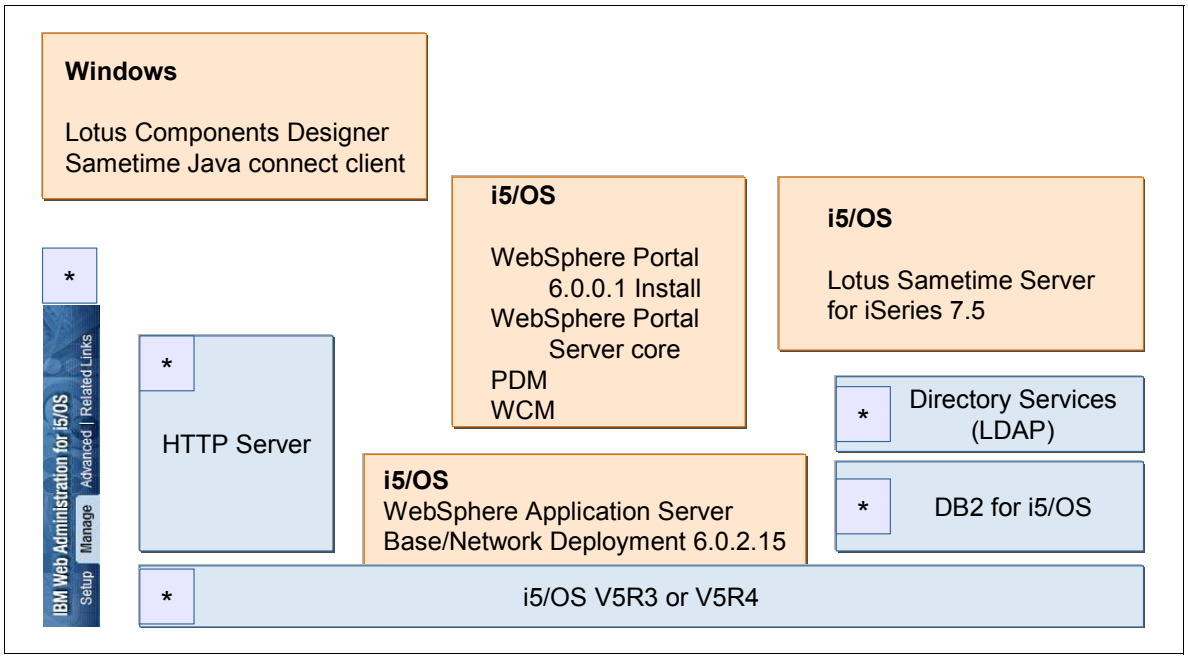


Figure 1-3 WebSphere Portal Express packaging on i5/OS

1.4 Why use i5/OS as a platform for WebSphere Portal Express

There are several reasons why i5/OS is an excellent platform to run WebSphere Portal Express. In this section, we discuss a few of them.

1.4.1 Consolidation of different workloads in a single server

The work management capabilities of i5/OS make it possible to combine several different workloads or applications in a single system or LPAR partition. It is possible to tune the individual applications to achieve the desired throughput while utilizing CPU, memory, and disk efficiently.

Figure 1-4 on page 8 shows a typical portal deployment in an environment where each application is deployed in an individual server. The cost and complexity of managing the environment grow quickly with the number of servers, while the typical CPU utilization per server is fairly low (20%). You cannot share underutilized and idle resources.

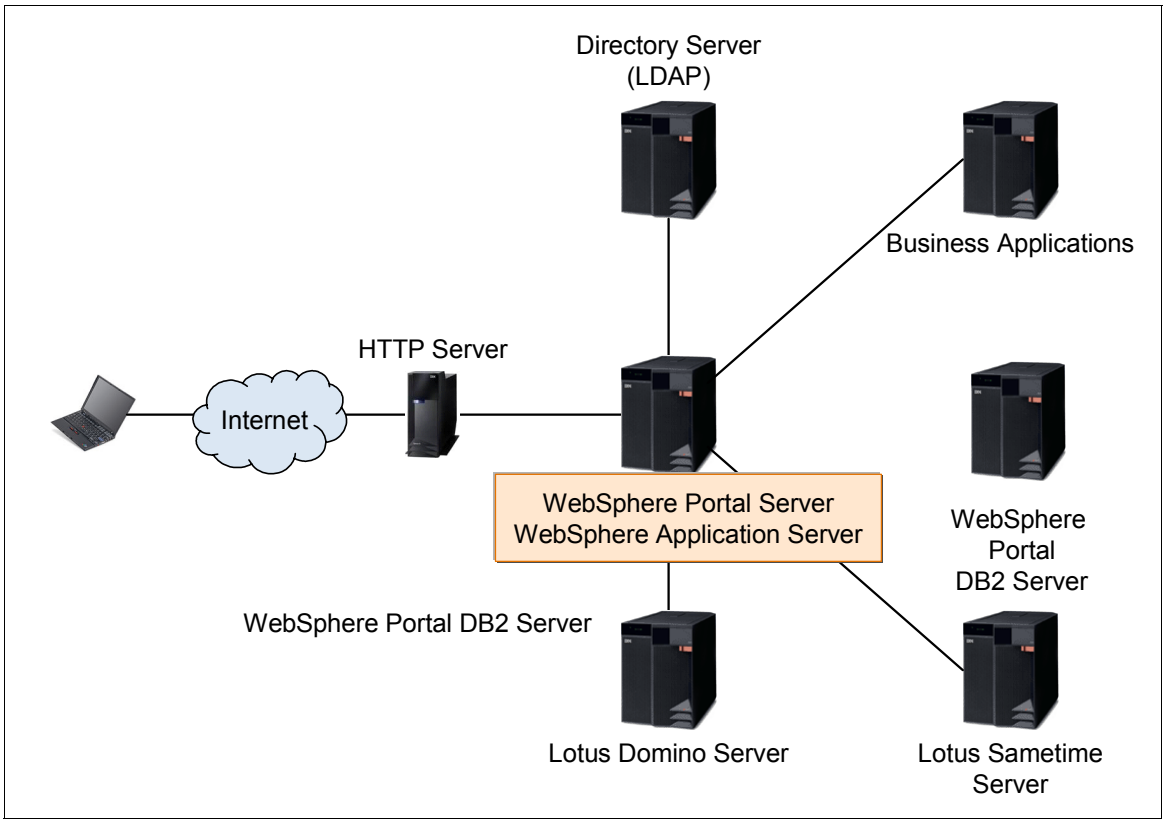


Figure 1-4 Typical portal deployment in a non-i5/OS platform

Figure 1-5 shows an example of WebSphere Portal Express deployment on i5/OS with WebSphere Portal, portal databases, business applications, and collaboration products all running in the same i5/OS environment.

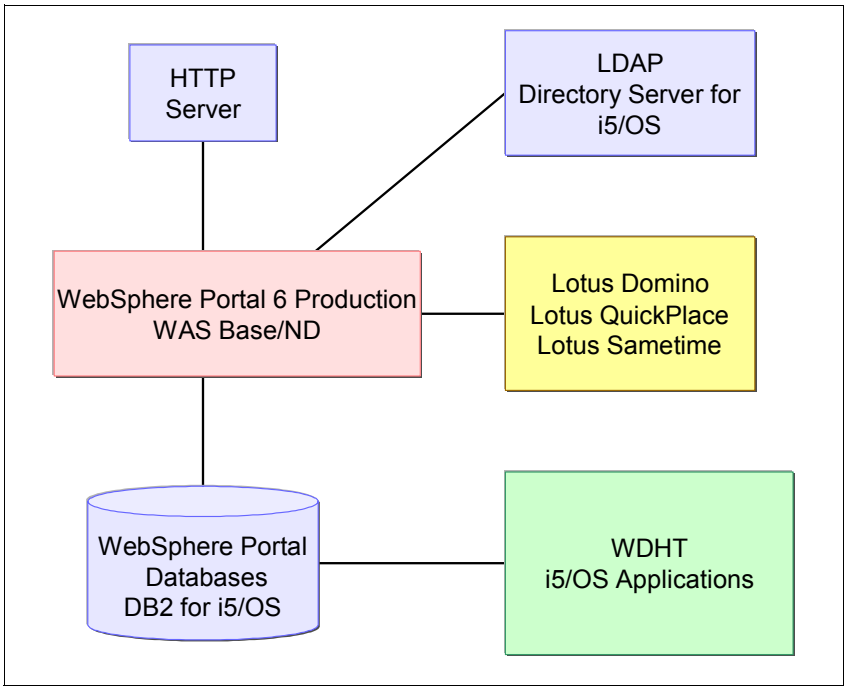


Figure 1-5 Typical portal deployment on i5/OS platform

Key benefits

The main benefits of workload consolidation are:

- Lower infrastructure and management cost
- Capability to share resources efficiently

1.4.2 Vertical scalability

The 64-bit operating system architecture and 64-bit JVM™ on i5/OS enable scalability on a single JVM. As the workload increases, it demands more memory and processing power. The 64-bit JVM enables i5/OS to increase the heap size as more memory is added. On System i, the portal workload can increase and is sustained by adding more memory and processing power to a single server.

In contrast, 32-bit operating systems have an address space limit of 4 GB, regardless of the amount of physical memory in the system. This limits the maximum size of each process in the system. In addition, several operating systems restrict the size of processes to even less than this limit. The approach to growth in those environments is by implementing horizontal clusters not only for high availability, but primarily for growth.

Key benefits

The main benefits of vertical scalability are:

- Higher workloads handled by a single server
- Simpler topology and easier to manage (horizontal clustering for growth is not required)

1.4.3 i5/OS exclusive functions for WebSphere Portal Express

Here are the functions that are unique to WebSphere Portal Express on i5/OS and not available on other platforms.

Portal configuration wizard in IBM Web Administration for i5/OS

System i clients expect integrated features that provide ease-of-use value. IBM developed, specifically for System i, a wizard driven configuration tool that is integrated into IBM Web Administration for i5/OS, which is shipped with the operating system and is regularly enhanced via PTFs (i5/OS fixes). This tool lets you create production-ready WebSphere Portal Express servers and WebSphere Portal Enterprise versions.

The wizard is started by clicking **Create WebSphere Portal** on the main IBM Web Administration for i5/OS page. The Configuration Wizard then walks the user through these steps:

1. Create and configure a new HTTP server instance.
2. Create a new WebSphere Application Server profile.
3. Configure WebSphere Portal, which includes adding WebSphere Portal to the WebSphere Application Server profile, DB2 for i5/OS configuration for WebSphere Portal, security enabled with LDAP, the configuration of Portal to work with Domino and extended products, and the deployment of portlets.

The wizard performs user input validation and verification of the infrastructure attributes up front. These are some of the verification examples performed by the wizard:

- Check prerequisite products and most recent PTFs.
- Validate LDAP type, ensuring that all the required attributes are in the LDAP directory.
- Detect TCP/IP ports in use to avoid port conflicts.
- Validate user IDs and passwords.

For more information about the Create WebSphere Portal wizard, see 3.2.2, “Configuring the WebSphere Portal profile” on page 73.

Through the IBM Web Administration for i5/OS, you can also manage your portal environment as follows:

- Start and stop the portal server and associated HTTP server.

  See 3.3.3, “Starting and stopping portal servers” on page 94 for more information.
- Access WebSphere Application Server and portal logs.

  See 3.2.3, “Accessing logs via IBM Web Administration for i5/OS” on page 87 for more information.
- Access WebSphere Administration Console for the portal profile.
- Delete a portal profile.

  See 3.5, “Deleting a WebSphere Portal Express profile” on page 101 for more information.
- Perform initial tuning.

  See Chapter 4, “Initial performance tuning” on page 105 for more information.

We use this wizard and administration functions in all of this Redpaper’s examples.

Backup and restore scripts

WebSphere Portal Express for i5/OS provides scripts to simplify offline backup and recovery of WebSphere Portal Express profiles. You can run the scripts manually from a QShell session or schedule them as part of a comprehensive backup and recovery strategy. The scripts save and restore all the components of the portal environment on i5/OS, including:

- The i5/OS integrated file system directory of the portal profile
- The external HTTP server associated with the portal profile
- All WebSphere Portal Express database libraries associated with the portal profile
- WebSphere registry data associated with the portal profile

Key benefits

The main benefits of the i5/OS exclusive features for WebSphere Portal Express are:

- Ease-of use, which reduces the skills and time required to perform the tasks
- Fewer errors and lower implementation cost because of infrastructure verification, input checking, and automation

For more information about backup and recovery, see Chapter 6, “Online backup and recovery” on page 241.

1.4.4 iSeries Access for Web portlets and single sign-on

iSeries Access for Web offers browser-based access to i5/OS. iSeries Access for Web enables users to leverage business information, applications, and resources across an enterprise by extending the System i resources to the client desktop through a Web browser.

If you run WebSphere Portal Express on i5/OS, you can integrate your System i resources with your portal environment using the iSeries Access for Web portlets. The available portlets and group of portlets are:

- 5250 portlet
- Integrated file system browsing portlets
- Printers, printer output, and output queue portlets
- Database tables and SQL portlets
- Commands portlets
- ZIP file portlet
- SSO access mapping the portal user to back-end i5/OS user profile

The iSeries Access for Web portlets are deployed automatically by the i5/OS Web portal configuration wizard described in 1.4.3, "i5/OS exclusive functions for WebSphere Portal Express" on page 9. Users can implement single sign-on (SSO) for i5/OS back-end user profiles using Enterprise Identity Mapping (EIM) and configure them using the i5/OS Web portal configuration wizard.

Key benefits

The main benefits of the iSeries Access for Web portlets are:

- Integrate System i back-end resources and applications in the portal environment with SSO.
- Provide Web access to i5/OS for users and system administrators through the portal single interface.

1.4.5 Running multiple portal profiles and versions in a single system

Multiple portal profiles can run in a single i5/OS environment. This allows you to implement a production environment and test portal environments in a single i5/OS partition. You can also install multiple versions of WebSphere Portal in the same i5/OS environment and create portal profiles that run different portal versions. This capability presents a lower cost alternative to running portal test environments on separate systems or LPAR partitions. However, it is not appropriate for all portal deployments, and you need to consider the drawbacks and benefits before making a decision about where to run your portal test environment.

These restrictions apply when running a portal test environment on the same i5/OS partition as the production environment:

- System sizing, especially memory, must take into account the test environment.
- Tune resource usage for each environment.
- Problems in one environment might affect the others.
- System PTFs affect all environments, but portal fix packs are applied to each portal profile independently of each other.
- Use extra caution with developer access rights.
- Need to schedule administrative tasks in the test environment to minimize performance impact on the production environment. Examples of test tasks that need to be scheduled during off-peak production hours are:
  - Installing products
  - Restarting servers
  - Creating and configuring new profiles
  - Applying fix packs

- Testing new developer code

Key benefits

The key benefits are:

- Less hardware and software expense to implement a portal test environment
- Good utilization of resources

1.4.6 i5/OS integration and low total cost of ownership

i5/OS is the industry leading *integrated* operating system. The i5/OS license entitles clients to these products and functions:

- DB2 for i5/OS, SQL compliant database, and database administration tools
- WebSphere Application Server Express, industry leading Web application server
- IBM HTTP server
- Communications and networking
- Major TCP/IP applications, protocols, and services:
  - LDAP
  - Telnet
  - FTP
  - NetServer™
  - SMTP
  - DNS
  - DHCP
  - IP filtering and Network Address Translation (NAT)
  - VPN
  - Intrusion detection
  - BOOTP
  - RoutD
- File serving
- Built-in security and tools for easy and low cost security implementation and auditing
- Single level storage and storage management
- Clustering and high availability
- Virtualization, workload management, and LPAR
- GUI and command line interfaces
- iSeries Access (included in the System i model 515 and 525 i5/OS license)

i5/OS all-in-one integration contributes to its legendary reliability, ease of management, security, and record uptime. Figure 1-6 on page 13 depicts the integrated nature of the i5/OS operating system.

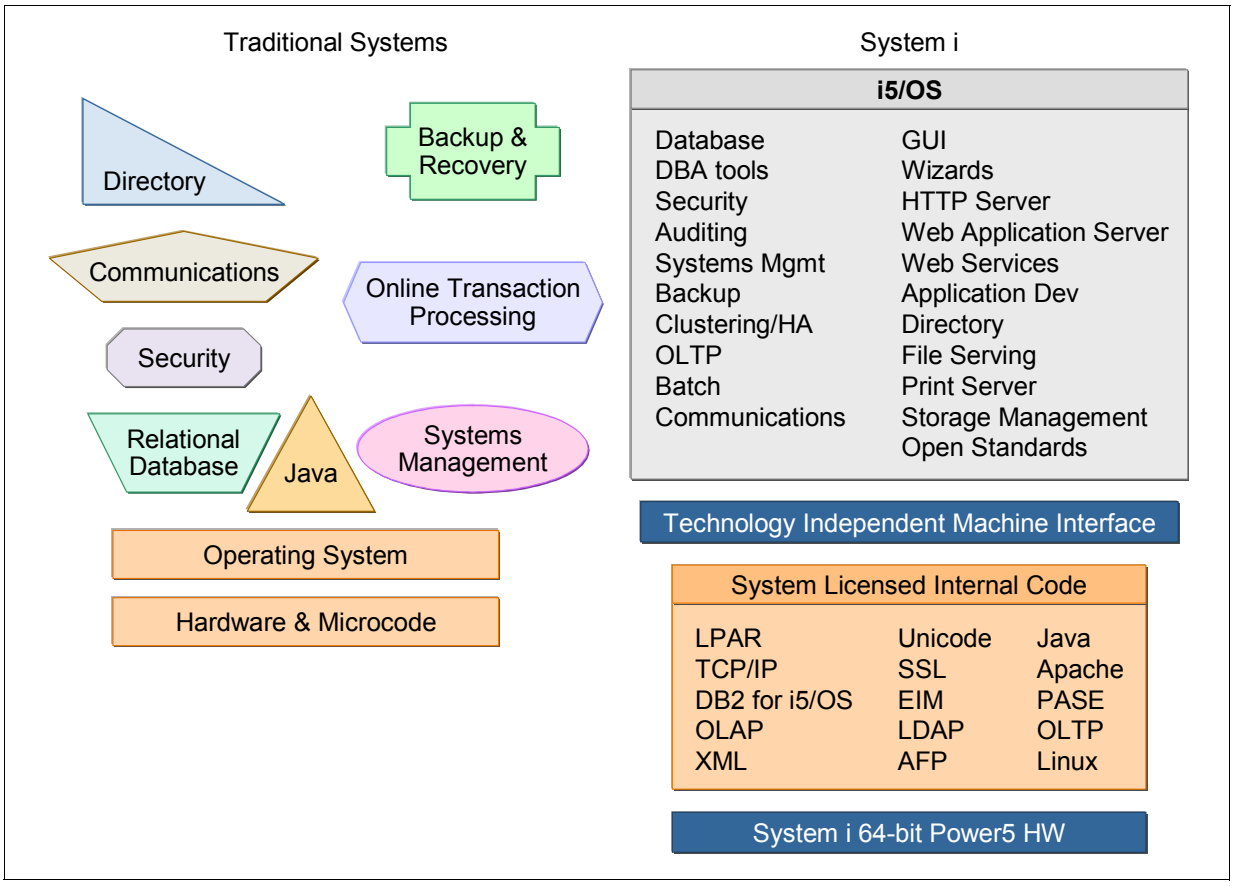


Figure 1-6 i5/OS: Leading integrated operating system and software license

Key benefits

The key benefits are:

- Low total cost of ownership (TCO) because of integration, ease of management, and consolidation
- Reliability, record uptime, and high client satisfaction

For more information about i5/OS benefits, analysts' reports, and client success stories, see the i5/OS Web site at:

`http://www.ibm.com/systems/i/os/i5os/`

1.4.7 Benefits for existing System i clients

In addition to the reasons listed in the previous sections, existing System i clients will experience these benefits by running WebSphere Portal on i5/OS:

- Leverage their existing investment in hardware, software, and skills.
- Use the same processes and tools for backup and restore procedures. For example, online backups of WebSphere Portal Express are also possible using Backup, Recovery, and Media Services (BRMS) for i5/OS.
- Include WebSphere Portal in your high availability strategy.
- Include WebSphere Portal in existing security procedures.

1.5 System i models for WebSphere Portal Express

IBM has announced several System i models that offer outstanding price/performance to run WebSphere and collaboration applications, such as WebSphere Portal Express. This section summarizes the System i models that are suitable for WebSphere Portal Express. Consult with your IBM sales representative or IBM Business Partner for more information:

- *System i 515 Express*: For small businesses with fewer than 40 users who are tired of dealing with the challenges of Microsoft Windows-based servers. This model is easy-to-manage, easy-to-secure, and a highly reliable alternative to Windows-based servers. For more information, see the IBM System i 515 Express Web site at:

  `http://www.ibm.com/systems/i/hardware/515/index.html`

- *System i 525 Express*: For small to mid-sized businesses, the System i 525 Express is ideal for companies that need an affordable, easy to use system with increased expansion options and easy upgrades with Capacity on Demand. Unlike Windows-based servers, the System i Express models are typically used to run multiple business applications on the same system. For more information, see the IBM System i 525 Express Web site at:

  `http://www.ibm.com/systems/i/hardware/525/index.html`

- *System i 520 Collaboration Edition*: For small and medium businesses deploying robust collaboration applications built on IBM Lotus Domino and IBM WebSphere Portal solutions. For more information, see the IBM System i 520 Collaboration Edition Web site at:

  `http://www.ibm.com/systems/i/hardware/520collaboration/`

- *System i 550 Domino edition*: For mid-size businesses deploying robust collaboration applications built on IBM Lotus Domino and IBM WebSphere Portal solutions. For more information, see the IBM System i Domino Edition Web site at:

  `http://www.ibm.com/servers/eserver/iseries/domino/edition.html`

- *i5/OS Application Server license*: This new i5/OS option is designed for application serving in partitions, where the applications do not require DB2 or are not required to access DB2 in another LPAR. An example is WebSphere Portal running in an i5/OS Application Server partition and accessing the portal databases in another LPAR partition running DB2 for i5/OS. This offering is available in System i models 550, 570, and 595. For more information, see the IBM announcement letter at:

  `http://www.ibm.com/common/ssi/fcgi-bin/ssialias?infotype=an&subtype=ca&htmlfid=897/ENUS207-068&appname=usn`

2

Preparing your i5/OS environment for WebSphere Portal Express

This chapter provides information about the prerequisite products and basic System i configuration that needs to be done before installing and configuring WebSphere Portal Express V6.0 on i5/OS. This chapter discusses the following topics:

- “Sizing the system” on page 16
- “Downloading the WebSphere Portal Express images” on page 16
- “Assembling the WebSphere Portal Express images” on page 20
- “i5/OS configuration and network requirements” on page 21
- “i5/OS software requirements” on page 29
- “Program temporary fixes” on page 32
- “Installing WebSphere Application Server” on page 36
- “Preparing the IBM Directory Server for i5/OS” on page 39

WebSphere Portal Express provides many installation and configuration options that are not discussed in this Redpaper. This Redpaper helps you get started quickly with a simple deployment example. For information about other planning considerations and topologies, see the WebSphere Portal V6 Information Center at:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp

© Copyright IBM Corp. 2007. All rights reserved.

2.1 Sizing the system

The minimum hardware requirements for WebSphere Portal Express V6 on i5/OS are:

Processor	POWER5™ System i models with at least 3800 CPW. Production environments need to consider servers with a higher commercial processing workload (CPW) rating.
Physical memory	5 GB at a minimum. Production environments and environments featuring multiple profiles require more memory.
Disk	A minimum of 6 disk arms is recommended.

You *must* properly size your System i machine before deploying WebSphere Portal Express. The following sizing resources are available:

- Workload Estimator

  http://www-912.ibm.com/wle/EstimatorServlet

- IBM Techline (IBM intranet):
  - IBM Techline Americas

    http://w3.ibm.com/support/americas/techline/

  - IBM Techline Europe

    http://w3.ibm.com/support/emea/techline/index.html

  - Techline Access for Business Partners

    http://ibm.com/partnerworld/techline

Environments supporting a limited number of users and tolerating longer server initialization can use systems that do not meet the recommended minimum requirements.

2.2 Downloading the WebSphere Portal Express images

Each platform (i5/OS, Windows, or Linux®) package is called an *assembly*. The eAssembly has its own part number and contains multiple downloadable electronic images (*eimages*). The *WebSphere Portal Express V6.0 Downloadable Files* document describes how to download and assemble WebSphere Portal Express Version 6.0. You can access the *WebSphere Portal Express V6.0 Downloadable Files* document at:

http://www.ibm.com/support/docview.wss?rs=688&uid=swg24014177

Table 2-1 on page 17 shows the part numbers and corresponding description for WebSphere Portal Express V6 and product prerequisites. The instructions in this chapter are limited to downloading only the WebSphere Portal Express and WebSphere Application Server product images. The *WebSphere Portal Express V6.0 Downloadable Files* document includes information about all the parts included in the i5/OS eAssembly.

The part number for the WebSphere Portal Express V6 for i5/OS is CR4W3ML.

Table 2-1 WebSphere Portal Express eimage part numbers

Part number	Description
C97Q3ML	IBM WebSphere Portal Express Quick Start and Server Install, V6.0 - Setup
C97Q6ML	IBM WebSphere Portal Express (Disc 1 of 2)
C97Q7ML	IBM WebSphere Portal Express (Disc 2 of 2)
C97Q8ML	IBM WebSphere Portal Express, V6.0
C97QBML	IBM WebSphere Application Server Base V6.0.2.9 for i5/OS
C97QCML	IBM WebSphere Application Server Network Deployment V6.0.2.9 for i5/OS

Note: In the example shown in this Redpaper, we configure the WebSphere Portal Express profile on WebSphere Application Server Base. We ordered the most recent WebSphere Application Server PTF group from IBM and did not use the eimages PTF group that is included in the WebSphere Portal Express eAssembly.

Perform the following steps to download the WebSphere Portal Express V6 eimages for i5/OS:

1. Create a directory on your local PC workstation where you will store the downloaded eimages. For example:

   `c:\PortalExpress6001`

2. Access one of the following software download Web sites and navigate to the software downloads page:
   - Download for IBM internal - Extreme Leverage at:

     `http://w3-103.ibm.com/software/xl/portal`
   - Download for IBM Business Partners - IBM Software Access Catalog at:

     `http://www.developer.ibm.com/isv/welcome/softmall.html`
   - Download for IBM clients - IBM Passport Advantage® at:

     `http://www-306.ibm.com/software/howtobuy/passportadvantage/`

3. You can download one eimage at a time by clicking **Find by part number** and entering the part number that you want to download. For example, to download the *IBM WebSphere Portal Express Quick Start and Server Install, V6.0 - Setup* eimage, enter `C97Q3ML` as the search argument (Figure 2-1). Repeat this step for all the eimages that you want to download.

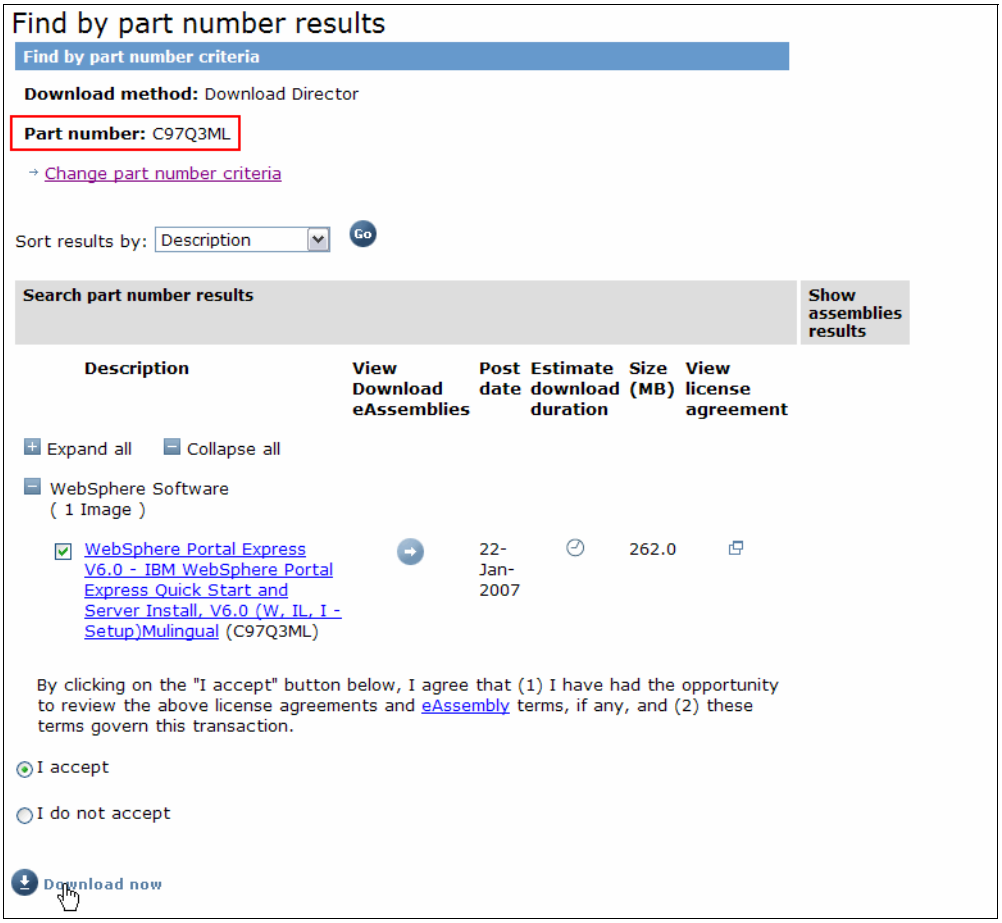

Find by part number results
Find by part number criteria
Download method: Download Director
Part number: C97Q3ML
Change part number criteria
Sort results by: Description
Go
Search part number results
Show assemblies results
Description
View Download eAssemblies
Post date
Estimate download duration
Size (MB)
View license agreement
Expand all
Collapse all
WebSphere Software
(1 Image)
WebSphere Portal Express V6.0 - IBM WebSphere Portal Express Quick Start and Server Install, V6.0 (W, IL, I - Setup)Mulingual (C97Q3ML)
22-Jan-2007
262.0
By clicking on the "I accept" button below, I agree that (1) I have had the opportunity to review the above license agreements and eAssembly terms, if any, and (2) these terms govern this transaction.
I accept
I do not accept
Download now

Figure 2-1 Finding by part number: Downloading a single eimage

4. You can also download all of the eimages at once by clicking **Find by part number** and entering the WebSphere Portal Express V6.0 for i5/OS eAssembly part number (CR4W3ML). Expand the eAssembly and select the eimages that you want to download. See Figure 2-2 and Figure 2-3.

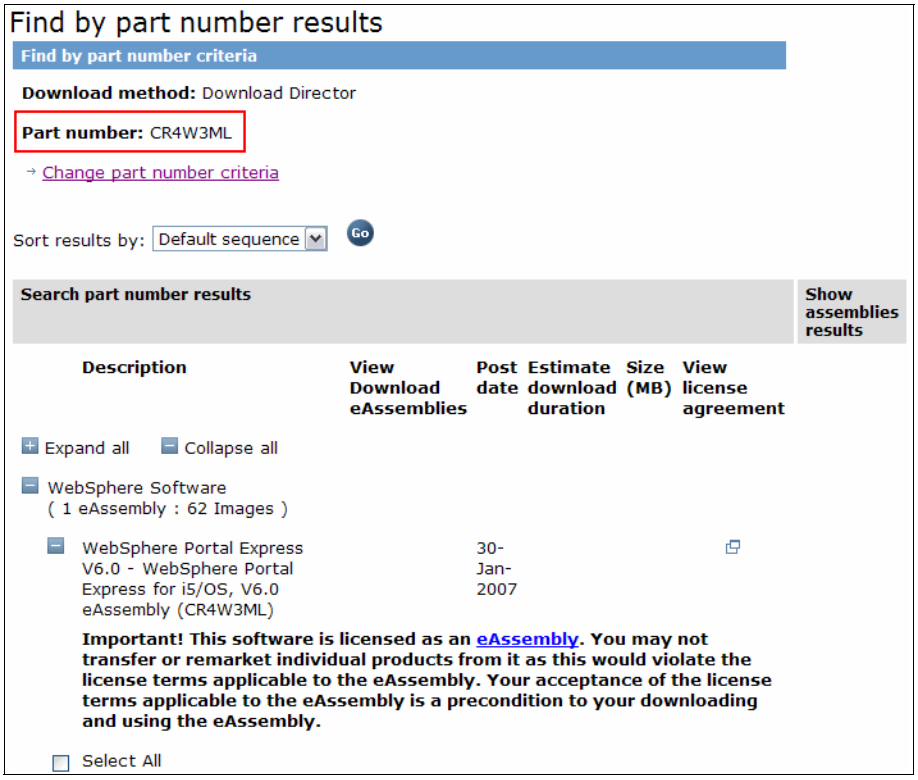

Find by part number results
Find by part number criteria
Download method: Download Director
Part number: CR4W3ML
Change part number criteria
Sort results by: Default sequence
Go
Search part number results
Show assemblies results
Description
View Download eAssemblies
Post date
Estimate download duration
Size (MB)
View license agreement
Expand all
Collapse all
WebSphere Software
(1 eAssembly : 62 Images)
WebSphere Portal Express V6.0 - WebSphere Portal Express for i5/OS, V6.0 eAssembly (CR4W3ML)
30-Jan-2007
Important! This software is licensed as an eAssembly. You may not transfer or remarket individual products from it as this would violate the license terms applicable to the eAssembly. Your acceptance of the license terms applicable to the eAssembly is a precondition to your downloading and using the eAssembly.
Select All

Figure 2-2 Finding by part number: Downloading multiple eimages in the eAssembly (1 of 2)

WebSphere Portal Express V6.0 - IBM WebSphere Portal Express Quick Start and Server Install, V6.0 (W, IL, I - Setup)Mulingual (C97Q3ML)
22-Jan-2007
262.0
WebSphere Portal Express V6.0 - IBM WebSphere Application Server Base for i5/OS, V6.0.2.9 (I-1) Multilingual (C97QBML)
22-Jan-2007
461.0
WebSphere Portal Express V6.0 - IBM WebSphere Application Server Network Deployment for i5/OS, V6.0.2.9 (I-2)Multilingual (C97QCML)
22-Jan-2007
468.0
WebSphere Portal Express V6.0 - IBM WebSphere Portal Express (1 of 2), V6.0 (W-3, IL-3, I-3)Multilingual (C97Q6ML)
22-Jan-2007
601.0
WebSphere Portal Express V6.0 - IBM WebSphere Portal Express (2 of 2), V6.0 (W-4, IL-4, I-4)Multilingual (C97Q7ML)
22-Jan-2007
466.0

Figure 2-3 Finding by part number: Downloading multiple eimages in the eAssembly (2 of 2)

2.3 Assembling the WebSphere Portal Express images

In this section, you assemble the eimages that you downloaded in 2.2, “Downloading the WebSphere Portal Express images” on page 16.

2.3.1 Assembling the WebSphere Application Server product

Perform the following steps to assemble the eimages for the WebSphere Application Server prerequisite:

1. Create a subdirectory under the download directory on your PC workstation to store the WebSphere Application Server prerequisites. In our example, we moved the WebSphere Application Server Base eimages to the `c:\PortalExpress6001\WAS_Prereqs` subdirectory as shown in Figure 2-4.

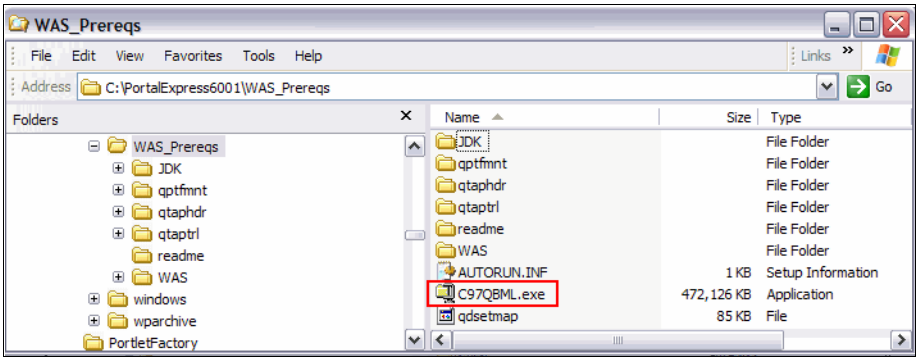


Figure 2-4 WebSphere Application Server Base eimages

2. Extract the electronic images for the WebSphere Application Server product version that you want to install (Base or Network Deployment). Refer to Table 2-1 on page 17 for a list of part numbers. In our example, the WebSphere Application Server directory was created by unzipping C97QBML.exe.

2.3.2 Assembling WebSphere Portal Express

The instructions in this section assume that you have downloaded the WebSphere Portal Express production electronic media to your local PC hard drive in a download directory, for example, `c:\PortalExpress6001`, as described in 2.2, “Downloading the WebSphere Portal Express images” on page 16.

To assemble the downloaded WebSphere Portal Express V6 product images, extract the following zip files using WinZip or an equivalent software product:

- C97Q3ML.zip
- C97Q6ML.zip
- C97Q7ML.zip
- C97Q8ML.zip

Figure 2-5 on page 21 shows the directory structure after unzipping the WebSphere Portal Express electronic images in the download directory.

Important: Unzip all the files to the same directory. Verify that all the zip files were extracted successfully. Failure to do so will lead to problems at installation time.

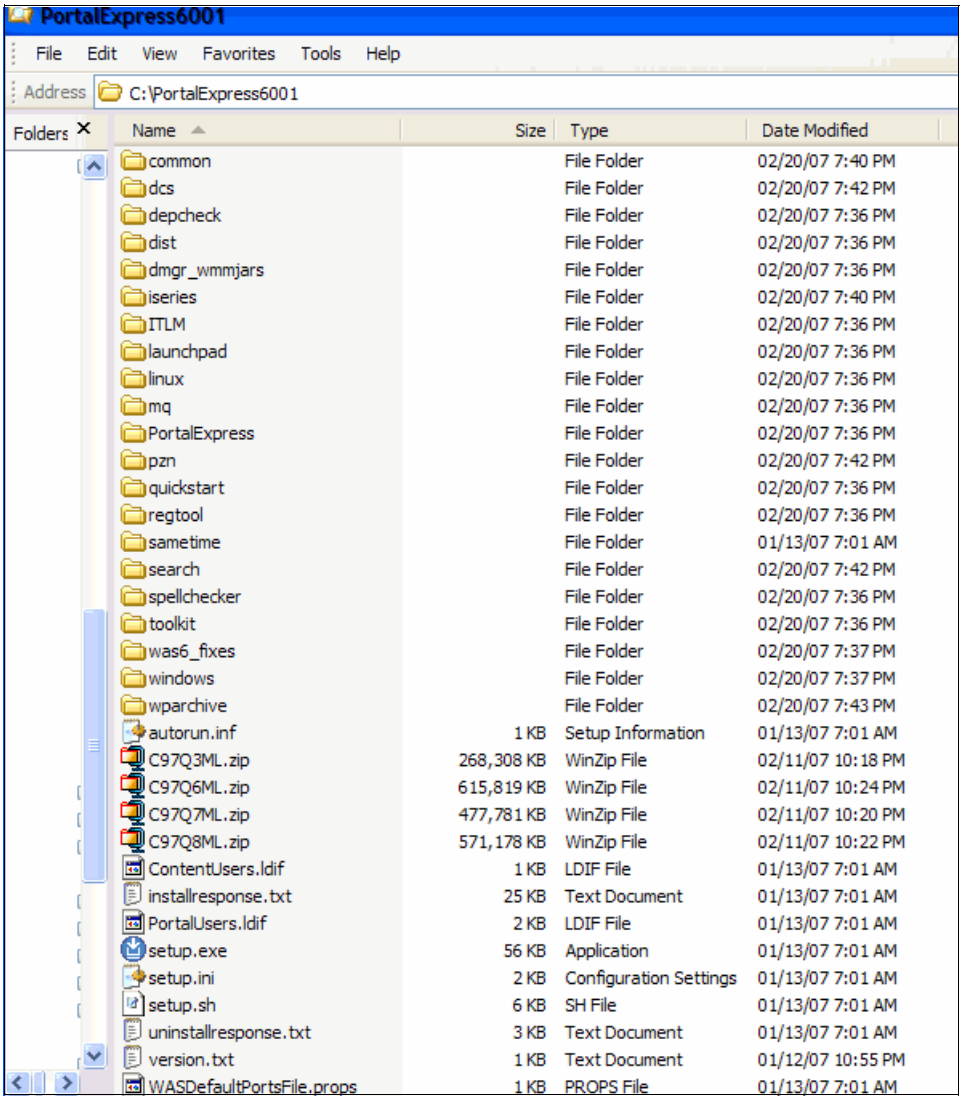

PortalExpress6001
File Edit View Favorites Tools Help
Address C:\PortalExpress6001
Folders
Name Size Type Date Modified
common File Folder 02/20/07 7:40 PM
dcs File Folder 02/20/07 7:42 PM
depcheck File Folder 02/20/07 7:36 PM
dist File Folder 02/20/07 7:36 PM
dmgr_wmmjars File Folder 02/20/07 7:36 PM
iseries File Folder 02/20/07 7:40 PM
ITLM File Folder 02/20/07 7:36 PM
launchpad File Folder 02/20/07 7:36 PM
linux File Folder 02/20/07 7:36 PM
mq File Folder 02/20/07 7:36 PM
PortalExpress File Folder 02/20/07 7:36 PM
pzn File Folder 02/20/07 7:42 PM
quickstart File Folder 02/20/07 7:36 PM
regtool File Folder 02/20/07 7:36 PM
sametime File Folder 01/13/07 7:01 AM
search File Folder 02/20/07 7:42 PM
spellchecker File Folder 02/20/07 7:36 PM
toolkit File Folder 02/20/07 7:36 PM
was6_fixes File Folder 02/20/07 7:37 PM
windows File Folder 02/20/07 7:37 PM
wparchive File Folder 02/20/07 7:43 PM
autorun.inf 1 KB Setup Information 01/13/07 7:01 AM
C97Q3ML.zip 268,308 KB WinZip File 02/11/07 10:18 PM
C97Q6ML.zip 615,819 KB WinZip File 02/11/07 10:24 PM
C97Q7ML.zip 477,781 KB WinZip File 02/11/07 10:20 PM
C97Q8ML.zip 571,178 KB WinZip File 02/11/07 10:22 PM
ContentUsers.ldif 1 KB LDIF File 01/13/07 7:01 AM
installresponse.txt 25 KB Text Document 01/13/07 7:01 AM
PortalUsers.ldif 2 KB LDIF File 01/13/07 7:01 AM
setup.exe 56 KB Application 01/13/07 7:01 AM
setup.ini 2 KB Configuration Settings 01/13/07 7:01 AM
setup.sh 6 KB SH File 01/13/07 7:01 AM
uninstallresponse.txt 3 KB Text Document 01/13/07 7:01 AM
version.txt 1 KB Text Document 01/12/07 10:55 PM
WASDefaultPortsFile.props 1 KB PROPS File 01/13/07 7:01 AM

Figure 2-5 Directory structure after extracting WebSphere Portal Express eimages

2.4 i5/OS configuration and network requirements

This section explains the i5/OS configuration and network requirements.

2.4.1 Verifying the i5/OS time zone

Before you install the WebSphere Portal Express software, make sure the time zone system value is set correctly for your system's time zone. The i5/OS system value of QTIMZON specifies the time zone information used to calculate the local system time.

You can verify the current time zone setting by using the following Work with System Values (WRKSYSVAL) CL command:

```
WRKSYSVAL SYSVAL(QTIMZON)
```

If you change the QTIMZON system value on the Work with System Values (WRKSYSVAL) display, type option 2 (Change) next to the QTIMZON system value and press Enter. On the Change System Value display (Figure 2-6), you can change the time zone value.

For a complete list of time zone values, see the Time zone topic in the System i Information Center at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzati/rzatitimezone.htm

```
                              Change System Value

System value . . . . . :   QTIMZON
Description  . . . . . :   Time zone

Type choice, press Enter.

  Time zone  . . . . . .   QN0600CST      Name

Associated settings:
  Offset . . . . . :   -06:00
  Full name  . . . :   Central Standard Time
  Abbreviated name :   CST

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel
```

Figure 2-6 Changing the QTIMZON system value

You also need to verify that the system's time is set correctly by verifying the QTIME system value.

2.4.2 Verifying the Coded Character Set Identifier

When configuring WebSphere Portal Express to work with DB2 UDB for i5/OS, it is essential to change the Coded Character Set Identifier (CCSID) from the default value of 65535, which is not supported by DB2 UDB for i5/OS.

Query the current system value by typing the following Display System Value (DSPSYSVAL) CL command from an i5/OS command line:

```
DSPSYSVAL SYSVAL(QCCSID)
```

If the CCSID value shown is 65535, use the Change System Value (CHGSYSVAL) CL command to change the QCCSID system value to a value that reflects the language used by most of the system. For example, for U.S. English, type the following command:

```
CHGSYSVAL SYSVAL(QCCSID) VALUE(37)
```

Refer to Language identifiers and associated default CCSIDs in the System i Information Center for a list of valid CCSIDs.

2.4.3 Verifying language settings of system values and user profiles

The IBM Web Administration for i5/OS interface (also referred to as the *HTTP Admin server*) calls the WebSphere Portal Express configuration scripts using QShell. When running in QShell, you to need to set up environment settings for language translations to occur

correctly. For instance, you can run into problems when the QLOCALE system value is set to *NONE. It is essential to change the CCSID because the default value of 65535 is not supported by WebSphere Portal Express using DB2 UDB for i5/OS. See 2.4.2, “Verifying the Coded Character Set Identifier” on page 22 for details.

These environment settings are stored in i5/OS system values and user profiles. It is a best practice to define the environment settings in the system values and to refer to these values from the user profile.

Table 2-2 shows an example of the system value settings for a system in Germany with a primary language of 2929 for German. You can use the Work with System Values (WRKSYSVAL) CL command to verify and change the settings of the system values shown in Table 2-2.

Table 2-2 System values for the language settings of a German system

System value	Value
QCCSID	273
QLOCALE	/QSYS.LIB/DE_DE.LOCALE
QLANGID	DEU
QCNTRYID	DE

Set the QLANGID and QCTRYID system values according to your language. For a list of values, see the default system values for national language versions in the i5/OS V5R4 Information Center at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/nls/rbagsnatlangdefaultsysval.htm

For example, set the following values for a U.S. English system:

```
CHGSYSVAL SYSVAL(QLOCALE) VALUE('/QSYS.LIB/EN_US.LOCALE')
CHGSYSVAL SYSVAL(QLANGID) VALUE(ENU)
CHGSYSVAL SYSVAL(QCNTRYID) VALUE(US)
```

Sign off and sign back on to make sure the new system values are in effect. You also need to restart the HTTP *ADMIN server using the following commands:

```
ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

The i5/OS user profile QTMHHTTP (used in the jobs for the HTTP ADMIN server) and the user profile you use when starting the IBM Web Administration for i5/OS refer to the settings defined in the system values as described. Table 2-3 shows the parameters of a user profile that are important in this context. The value *SYSVAL refers to the values that are set in the system values.

Verify that the two user profiles have the correct values for your environment.

Use the Display User Profile (DSPUSRPRF) CL command to verify the settings for the values shown in Table 2-3.

Table 2-3 i5/OS user profile language parameters

Description	Parameter Name	Value
Language ID	LANGID	*SYSVAL
Country or region ID	CNTRYID	*SYSVAL
Coded character set ID	CCSID	*SYSVAL
Locale	LOCALE	*SYSVAL

2.4.4 Network requirements

Configuring a WebSphere Portal Express server on i5/OS requires a static TCP/IP address and a fully qualified host name. Before you start configuring a WebSphere Portal Express server, determine the dedicated static TCP/IP address and the fully qualified host name to use.

Note: You can associate your portal profile with a TCP/IP host name and IP address that is different from the local system host name.

Determining the availability of a static TCP/IP address

WebSphere Portal Express server on i5/OS requires the use of a static TCP/IP address. Perform the following steps to determine an available TCP/IP address:

1. From an i5/OS command line, enter the Configure TCP/IP (CFGTCP) CL command and press Enter.
2. On the Configure TCP/IP menu, type option 1 (Work with TCP/IP interfaces) and press Enter.
3. On the Work with TCP/IP Interfaces display shown in Figure 2-7, all the currently configured TCP/IP addresses are displayed. From here, you have the options to add, change, remove, display, start, or end the TCP/IP interfaces.

Note: Verify that the *LOOPBACK entry exists in your system as shown in Figure 2-7. You *must* also have at least one TCP/IP address, other than 127.0.0.1, defined on your system.

```
                        Work with TCP/IP Interfaces
                                                              System:   RCHAS10
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet              Line      Line
Opt  Address          Mask             Description  Type

     10.10.10.1       255.255.255.128  ETHLINE      *ELAN
     10.10.10.2       255.255.255.128  ETHLINE      *ELAN
     10.10.10.3       255.255.255.128  ETHLINE      *ELAN
     127.0.0.1        255.0.0.0        *LOOPBACK    *NONE

                                                                      Bottom
F3=Exit      F5=Refresh   F6=Print list   F11=Display interface status
F12=Cancel   F17=Top      F18=Bottom
```

Figure 2-7 Work with TCP/IP Interfaces display

Verifying the fully qualified host name

Each WebSphere Portal server profile requires a static TCP/IP address and a fully qualified host name. If the host name is listed in the i5/OS host table, the fully qualified host name is required to be the first item listed after the IP address.

Along with the i5/OS host table, adding the fully qualified host name to your Domain Name System (DNS) server or servers ensures remote and client name resolution.

Note: We recommend that you update the i5/OS local host table with the fully qualified host name of the WebSphere Portal server. The name resolution of the portal server by a DNS server is also a supported configuration. The host and domain names in the host table and DNS are case-sensitive.

Perform the following steps to verify whether your system is configured with a fully qualified host name:

1. From an i5/OS command line, enter the Configure TCP/IP (CFGTCP) CL command and press Enter.
2. On the Configure TCP/IP menu, type option `12` (Change TCP/IP domain information) and press Enter.
3. On the Change TCP/IP Domain (CHGTCPDMN) display, verify the fully qualified host name of your system. In Figure 2-8, the fully qualified host name in our example is `RCHAS10.RCHLAND.IBM.COM`.

Tip: Specify the Host name search priority parameter as `*LOCAL` and add the WebSphere Portal TCP/IP host name to the i5/OS host table, even if you have a DNS.

Note: If you are changing the TCP/IP domain, you might need to IPL the system.

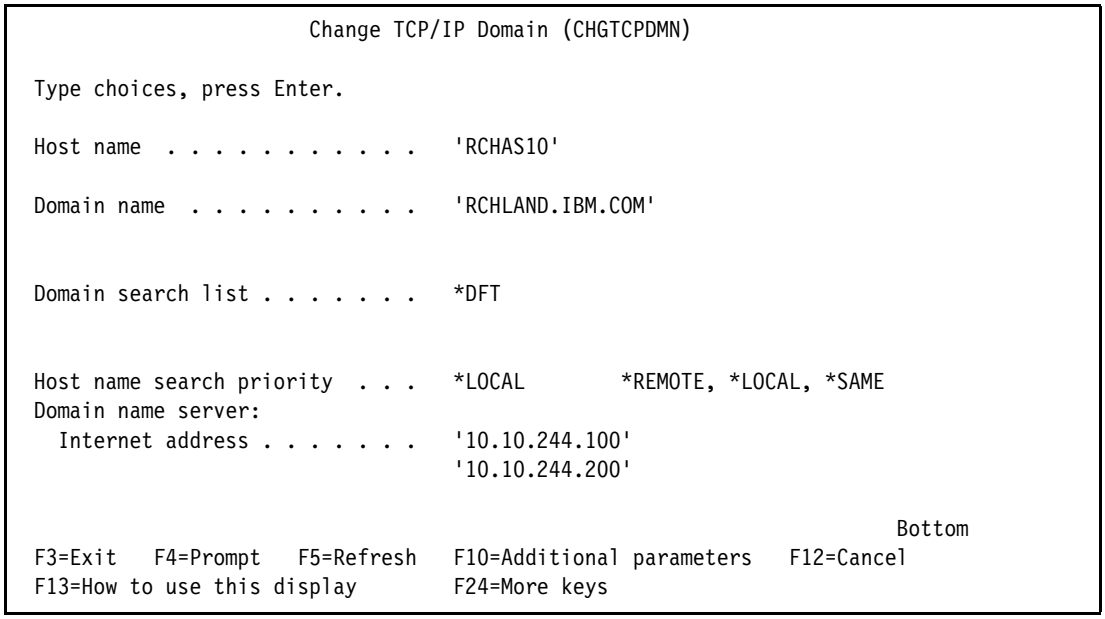

Change TCP/IP Domain (CHGTCPDMN)
Type choices, press Enter.
Host name . . . . . 'RCHAS10'
Domain name . . . . . 'RCHLAND.IBM.COM'
Domain search list . . . . . *DFT
Host name search priority . . . *LOCAL *REMOTE, *LOCAL, *SAME
Domain name server:
Internet address . . . . . '10.10.244.100'
'10.10.244.200'
Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

Figure 2-8 Verifying the fully qualified host name of the system

Updating the i5/OS local host table

Using an available static TCP/IP address and a fully qualified host name for the WebSphere Portal server, perform the following steps to update the i5/OS local host table:

1. From an i5/OS command line, enter the Configure TCP/IP (CFGTCP) CL command and press Enter.
2. On the Configure TCP/IP menu, type option `10` (Work with TCP/IP host table entries) and press Enter.
3. On the Work with TCP/IP Host Table Entries display, type option `1` (Add) and press Enter.
4. On the Add TCP/IP Host Table Entry (ADDTCPHTE) display, type the TCP/IP address with the fully qualified host name listed *first*.

   Figure 2-9 shows an example of the host table entries for a WebSphere Portal Express server called `ITSOWPE1`. Notice that the fully qualified host name is added first.

Note: Specify the fully qualified host name for the TCP/IP host before the non-fully qualified name. The host and domain names in the host table and DNS are case-sensitive.

```
                      Add TCP/IP Host Table Entry (ADDTCPHTE)

Type choices, press Enter.

Internet address . . . . . . . . > '10.10.10.1'
Host names:
Name . . . . . . . . . . . . . . > ITSOWPE1.RCHLAND.IBM.COM
Name . . . . . . . . . . . . . . > ITSOWPE1

Text 'description' . . . . . .   'IBM WebSphere Portal Express server'

                                                                        Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Figure 2-9 Adding a TCP/IP host table entry

5. Confirm that the fully qualified host name resolves to the correct IP address by typing the following PING CL command from an i5/OS command line:

   `ping ITSOWPE1.RCHLAND.IBM.COM`

   Replace `ITSOWPE1.RCHLAND.IBM.COM` with the fully qualified host name that you assigned to your WebSphere Portal server. See Figure 2-10.

```
                                Command Entry                          RCHAS10
                                                          Request level:   1
 Previous commands and messages:
    > ping ITSOWPE1.RCHLAND.IBM.COM
      Verifying connection to host system ITSOWPE1.RCHLAND.IBM.COM at address
       10.10.10.1.
      PING reply 1 from 10.10.10.1 took 0 ms. 256 bytes. TTL 64.
      PING reply 2 from 10.10.10.1 took 0 ms. 256 bytes. TTL 64.
      PING reply 3 from 10.10.10.1 took 0 ms. 256 bytes. TTL 64.
      PING reply 4 from 10.10.10.1 took 0 ms. 256 bytes. TTL 64.
      PING reply 5 from 10.10.10.1 took 0 ms. 256 bytes. TTL 64.
      Round-trip (in milliseconds) min/avg/max = 0/0/0.
      Connection verification statistics: 5 of 5 successful (100 %).
                                                                        Bottom
 Type command, press Enter.
 ===>
F3=Exit   F4=Prompt   F9=Retrieve   F10=Include detailed messages
 F11=Display full      F12=Cancel    F13=Information Assistant   F24=More keys
```

Figure 2-10 Verifying the TCP/IP host table entry

Verifying the Relational Database Directory Entry

A database on other platforms correlates to a relational database (RDB) directory entry on i5/OS. Each system in the network that has a relational database *must* have a unique RDB directory entry name.

To verify your local database, from an i5/OS command line, type the Work with Relational Database Directory Entries (WRKRDBDIRE) CL command and press Enter. You see the Work with Relational Database Directory Entries display as shown in Figure 2-11.

```
               Work with Relational Database Directory Entries

 Position to  . . . . . .

 Type options, press Enter.
   1=Add   2=Change   4=Remove   5=Display details   6=Print details

                              Remote
 Option  Entry                Location                  Text

         RCHAS10              *LOCAL
```

Figure 2-11 Work with Relational Database Directory Entries (WRKRDBDIRE) display

If your system does not have a local RDB directory entry, it is important to provide a name that is resolved through TCP/IP on your network. We recommend that you provide the same name for the RDB directory entry name as the TCP/IP name of your system. Perform the following steps:

1. Use the i5/OS CL command of Display Network Attributes (DSPNETA) to obtain the TCP/IP name of your system. See Figure 2-12.

```
                         Display Network Attributes
                                                              System:   RCHAS10
 Current system name  . . . . . . . . . . . . . . . :   RCHAS10
   Pending system name  . . . . . . . . . . . . . . :
 Local network ID . . . . . . . . . . . . . . . . . :   APPN
 Local control point name . . . . . . . . . . . . . :   RCHAS10
 Default local location . . . . . . . . . . . . . . :   RCHAS10
 Default mode . . . . . . . . . . . . . . . . . . . :   BLANK
 APPN node type . . . . . . . . . . . . . . . . . . :   *ENDNODE
 Data compression . . . . . . . . . . . . . . . . . :   *NONE
 Intermediate data compression  . . . . . . . . . . :   *NONE
 Maximum number of intermediate sessions  . . . . . :   200
 Route addition resistance  . . . . . . . . . . . . :   128
 Server network ID/control point name . . . . . . . :   *LCLNETID   *ANY
                                                                       More...
 Press Enter to continue.
F3=Exit   F12=Cancel
```

Figure 2-12 Display Network Attributes (DSPNETA) display

2. Type the Add Relational Database Directory Entry (ADDRDBDIRE) CL command and press F4 to prompt the command, or type option 1 (Add) on the Work with Relational Database Directory Entries (WRKRDBDIRE) display to create a new entry. On the Add Relational Database Directory Entry (ADDRDBDIRE) display, enter the following parameters:
   - Relational database: TCP/IP name of your system found in Step 1 on page 26.
   - Name or address: *LOCAL. This identifies the entry as local to your system.
   - Type: *IP. This sets the use of the IP protocol for communication.

   Keep the default value of all the other parameters and press Enter. See Figure 2-13 on page 29.

```
                    Add RDB Directory Entry (ADDRDBDIRE)

Type choices, press Enter.

Entry:                            RDB
  Relational database  . . . . .              > RCHAS10
  Relational database alias  . .                *NONE
Remote location:                  RMTLOCNAME
  Name or address  . . . . . . .                *LOCAL

  Type . . . . . . . . . . . . .                *IP
Text . . . . . . . . . . . . . . TEXT           *BLANK

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 2-13 Adding a relational database directory entry

Note: There is no comparable function in the iSeries Navigator graphical interface to create a RDB directory entry.

2.5 i5/OS software requirements

Table 2-4 on page 30 lists the licensed program software for i5/OS that is required to run WebSphere Portal Express V6.

Important: The WebSphere Application Server version required by WebSphere Portal Express is Base or Network Deployment (ND) V6.0. Other versions of WebSphere Application Server can coexist on the same i5/OS partition, but you cannot use it instead of the required version. For example, you can have WebSphere Application Server Express V6.0 or WebSphere Application Server Base V6.1 installed. However, you *must* install WebSphere Application Server Base or ND V6.0 to satisfy WebSphere Portal Express V6 requirements.

If you already have the required WebSphere Application Server version on your system, you do not need to reinstall it. You only need to verify that the PTF group level is at the minimum required level as described in 2.6.1, “Required i5/OS V5R3 PTFs” on page 33 and 2.6.2, “Required i5/OS V5R4 PTFs” on page 33.

Table 2-4 i5/OS software requirements for WebSphere Portal Express V6

Licensed program product	Option	Description
5722-SS1	*BASE	OS/400® V5R3 or V5R4
	12	OS/400 - Host Servers
	30	OS/400 - Qshell Interpreter
	33	OS/400 - Portable Application Solution Environment (PASE)
	34	Digital Certificate Manager
	43	OS/400 - Additional Fonts
5722-AC3	*BASE	Cryptographic Access Provider 128-bit (V5R3 only)
5722-DG1	*BASE	IBM HTTP Server for i5/OS
5722-JC1	*BASE	IBM Toolbox for Java
5722-JV1	*BASE	IBM Developer Kit for Java
	5	Developer Toolkit 1.3
	6	Developer Toolkit 1.4
5733-W60	*BASE	WebSphere Application Server for OS/400 V6
	2	WebSphere Application Server V6 (“Base”) [1]
	3	WebSphere Application Server V6 Network Deployment [1]
5722-TC1	*BASE	TCP/IP Connectivity Utilities
5722-XW1	*BASE	IBM eServer™ iSeries Access Family[2] (optional)
5722-XH2	*BASE	iSeries Access for Web [2](optional)

1. Only one of the WebSphere Application Server V6 options 2 or 3 needs to be installed, even if you can install both. Option 2, WebSphere Application Server V6 (“Base”), is the only version supported by the IBM Create WebSphere Portal Wizard for i5/OS in IBM Web Administration for i5/OS.
2. iSeries Access for Web is required only if you want to give users access to existing i5/OS applications using the iSeries Access for Web portlets. It might need to be installed on additional systems running such applications. Note that 5722-XH2 V5R4 is required for portal integration. You can install 5722-XH2 V5R4 on i5/OS V5R3.

2.5.1 Displaying installed i5/OS software

To determine what i5/OS software is currently installed on your system, perform the following steps:

1. Sign on to a 5250 emulation session on your i5/OS instance.
2. Enter the Display Software Resources (DSPSFWRSC) CL command and press Enter.

3. On the Display Software Resources display (Figure 2-14), verify the software that is installed.

```
                        Display Software Resources
                                                              System: RCHAS10
Resource
   ID      Option  Feature  Description
5722999    *BASE    5050    Licensed Internal Code
5722SS1    *BASE    5050    Operating System/400
5722SS1    *BASE    2924    Operating System/400
5722SS1    1        5050    OS/400 - Extended Base Support
5722SS1    1        2924    OS/400 - Extended Base Support
5722SS1    2        5050    OS/400 - Online Information
5722SS1    2        2924    OS/400 - Online Information
5722SS1    3        5050    OS/400 - Extended Base Directory Support
5722SS1    3        2924    OS/400 - Extended Base Directory Support
5722SS1    12       5050    OS/400 - Host Servers
5722SS1    12       2924    OS/400 - Host Servers
5722SS1    30       5050    OS/400 - Qshell
5722SS1    30       2924    OS/400 - Qshell
5722SS1    31       5050    OS/400 - Domain Name System
                                                                       More...
Press Enter to continue.

F3=Exit   F11=Display libraries/releases   F12=Cancel
F19=Display trademarks
```

Figure 2-14 Display Software Resources

4. On the same display, press F11 (Display libraries/releases) to view the release level of the products installed. See Figure 2-15.

```
                        Display Software Resources
                                                          System: RCHAS12
Resource                    Feature
   ID      Option  Feature   Type    Library     Release
5722999    *BASE    5050     *CODE   QSYS        V5R4M0 L00
5722SS1    *BASE    5050     *CODE   QSYS        V5R4M0 L00
5722SS1    *BASE    2924     *LNG    QSYS        V5R4M0 L00
5722SS1    1        5050     *CODE   QSYS2       V5R4M0
5722SS1    1        2924     *LNG    QSYS2       V5R4M0
5722SS1    2        5050     *CODE   QHLPSYS     V5R4M0
5722SS1    2        2924     *LNG    QHLPSYS     V5R4M0
5722SS1    3        5050     *CODE   QSYSDIR     V5R4M0
5722SS1    3        2924     *LNG    QSYSDIR     V5R4M0
5722SS1    12       5050     *CODE   QIWS        V5R4M0
5722SS1    12       2924     *LNG    QIWS        V5R4M0
5722SS1    30       5050     *CODE   QSHELL      V5R4M0
5722SS1    30       2924     *LNG    QSHELL      V5R4M0
                                                                   More...
Press Enter to continue.

F3=Exit   F11=Display descriptions   F12=Cancel   F19=Display trademarks
```

Figure 2-15 Display Software Resources display showing the installed releases

You can also use iSeries Navigator to verify the currently installed licensed software on your system. From iSeries Navigator, click **My Connections** → ***systemname*** → **Configuration and Service** → **Software** → **Installed Products** as shown in Figure 2-16. The panel on the right shows the currently installed software on your system.

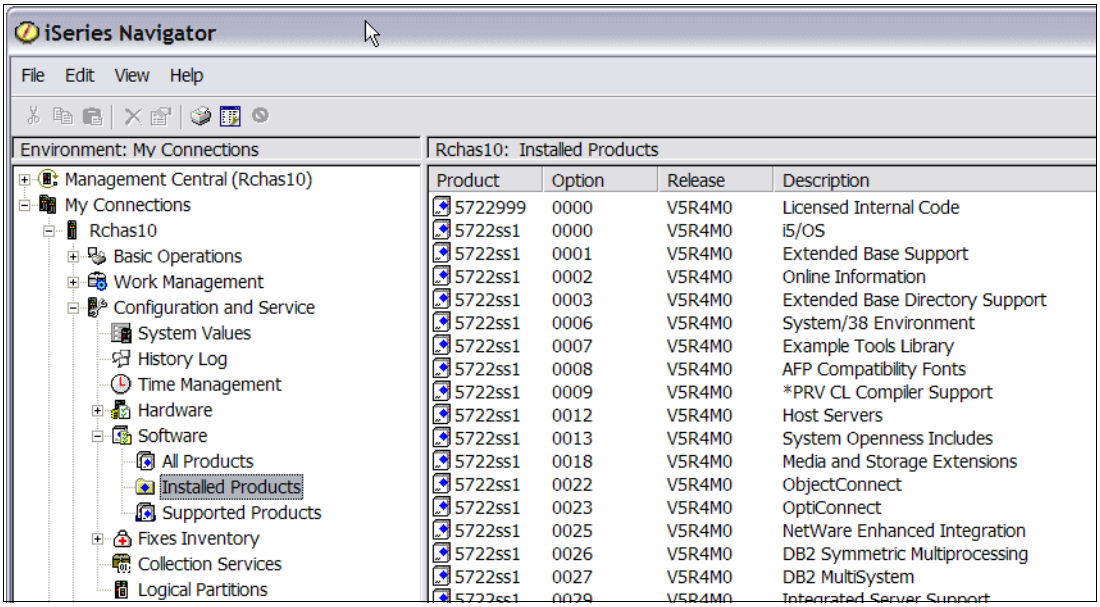


Figure 2-16 Using iSeries Navigator to display installed licensed software

2.6 Program temporary fixes

System updates and fixes on i5/OS are applied through a *Program Temporary Fix or PTF*. The PTFs that are required to be loaded on the system depend on the version and release of i5/OS that is used and the software products that are installed on the system. This section covers the minimum PTFs that are required to perform the configuration steps.

Note: Make sure that the latest i5/OS cumulative PTF package is installed.

Running IBM WebSphere Portal Express V6 for i5/OS requires both individual PTFs and group PTF packages. Each individual PTF and group PTF package usually includes specific installation instructions.

Also, the IBM Create WebSphere Portal Wizard for i5/OS verifies that the required individual and group PTFs are installed prior to configuring a portal server.

To order or download System i program temporary fixes (PTFs), see the following Web sites:

- Fix Central

  http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp

- System i Group PTFs

  http://www-912.ibm.com/s_dir/slineO03.NSF/GroupPTFs?OpenView&view=GroupPTFs

- Support for IBM System i

  http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/brandmain?brandind=5000027

2.6.1 Required i5/OS V5R3 PTFs

Install or verify the PTF groups listed in Table 2-5 for i5/OS V5R3. Ensure that WebSphere Application Server is installed before installing PTFs. It is a good practice to update the PTF level on your system to the latest level before installing WebSphere Portal Express. For the latest PTF Group information, see the Preventive Service Planning Web site at:

http://www-912.ibm.com/s_dir/slineO03.NSF/GroupPTFs

Table 2-5 Required i5/OS V5R3 group PTFs for WebSphere Portal Express

Group PTF	Description	Minimum level
SF99530	Cumulative PTF package	5298
SF99503	DB2 Universal Database™ for i5/OS	8
SF99301	WebSphere Application Server V6	16
SF99269	Java	9
SF99099	IBM HTTP Server for i5/OS	13[1]
SF99173	IBM Business Solutions (Only required if IBM Business Solutions (5722-BZ1) is installed.)	3
SF99295	WebSphere MQ for iSeries Version 5, Release 3 (Only required if WebSphere MQ for iSeries (5724-B41) is installed.)	11

1 SF99099 level 13 includes support for WebSphere Portal Express V6.0 configuration in IBM Web Administration for i5/OS.

You *must* install the following PTFs on your system before installing WebSphere Portal Express. Use the Display PTF (DSPPTF) CL command to verify that the PTF is installed or superseded:

- 5722-SS1: SI24550
- 5722-XH2: SI25551 (PTF is for 5722-XH2 V5R4, but you can install it on i5/OS V5R3.)
- 5722-DG1:
  - SI28182
  - SI27057 is only required for WebSphere Portal Express V6.0 support in IBM Web Administration for i5/OS.

Important: We recommend that you have all the latest PTFs for 5722-DG1 loaded on your system.

2.6.2 Required i5/OS V5R4 PTFs

Install or verify the PTF groups listed in Table 2-6 on page 34 for i5/OS V5R4. Ensure that WebSphere Application Server is installed before installing PTFs. It is a good practice to update the PTF level on your system to the latest level before installing WebSphere Portal Express. For the latest PTF Group information, see the Preventive Service Planning Web site at:

http://www-912.ibm.com/s_dir/slineO03.NSF/GroupPTFs

Table 2-6 Required i5/OS V5R4 group PTFs for WebSphere Portal Express

Group PTF	Description	Minimum level
SF99540	Cumulative PTF package	6024
SF99504	DB2 Universal Database for i5/OS	2
SF99312	WebSphere Application Server V6	6
SF99291	Java	2
SF99114	IBM HTTP Server for i5/OS	8[1]
SF99173	IBM Business Solutions (Required if IBM Business Solutions (5722-BZ1) is installed.)	3
SF99296	WebSphere MQ for iSeries Version 5, Release 3 (Required if WebSphere MQ for iSeries (5724-B41) is installed.)	5

1 SF99114 level 8 includes support for WebSphere Portal Express V6.0 configuration in IBM Web Administration for i5/OS.

You *must* install the following PTFs on your system before installing WebSphere Portal Express. Use the Display PTF (DSPPTF) CL command to verify that the PTF is installed or superseded.

- 5722999: MF40746, MF40747 (Both of these PTFs are not needed in V5R4M5.)

Note: PTFs MF40746 and MF40747 require an IPL of the system.

- 5722-SS1: SI24505, SI24569, SI24629, SI24864
- 5722-XH2: SI25551
- 5722-DG1:
  - SI28135
  - SI27058 is only required for WebSphere Portal Express V6.0 support in IBM Web Administration for i5/OS.

Important: We recommend that you have all the latest PTFs for 5722-DG1 loaded on your system.

2.6.3 Verifying group PTFs

To verify that the correct group PTF levels are installed on your system, perform the following steps:

1. Sign on to a 5250 emulation session on your i5/OS instance.
2. Enter the Work with PTF Groups (WRKPTFGRP) CL command on a command line and press Enter.

3. The Work with PTF Groups display (Figure 2-17) lists the group PTFs installed on your system and the level of the PTF. Verify that each group PTF shows a status of `Installed`.

> **Tip:** Verify the status of the PTF groups again immediately before the WebSphere Portal Express installation to ensure that all the PTF groups are in `Installed` status.

```
                          Work with PTF Groups
                                                          System:   RCHAS10
Type options, press Enter.
  4=Delete   5=Display   6=Print   8=Display special handling PTFs
  9=Display related PTF groups

Opt  PTF Group             Level  Status
     SF99540                6297  Installed
     SF99539                  38  Installed
     SF99504                   9  Installed
     SF99315                   5  Installed
     SF99312                  14  Installed
     SF99291                   7  Installed
     SF99143                   1  Installed
     SF99114                   8  Installed



                                                                       Bottom
F3=Exit   F6=Print   F11=Display descriptions   F12=Cancel
F22=Display entire field
```

Figure 2-17 Work with PTF Groups (WRKPTFGRP) initial display

4. The initial Work with PTF Groups display provides limited information. For a more descriptive display of the group PTF information, press F11 (Display descriptions) and you see the group PTF descriptions as shown in Figure 2-18.

```
                          Work with PTF Groups
                                                          System:   RCHAS12
 Type options, press Enter.
   4=Delete   5=Display   6=Print   8=Display special handling PTFs
   9=Display related PTF groups

 Opt  PTF Group             Text
      SF99530               CUMULATIVE PTF PACKAGE C4272530
      SF99503               DB2 UDB FOR ISERIES
      SF99287               WEBSPHERE APP SERVER V5.0 (BASE EDITION)
      SF99282               WEBSPHERE PORTAL EXPRESS/EXPRESS PLUS SERVICE PACK
      SF99269               JAVA
      SF99099               IBM HTTP SERVER FOR ISERIES

                                                                       Bottom
 F3=Exit   F6=Print   F11=Display status   F12=Cancel
 F22=Display entire field
```

Figure 2-18 Work with PTF Groups (WRKPTFGRP) display showing the descriptions

2.7 Installing WebSphere Application Server

For WebSphere Application Server installation instructions, see the WebSphere Application Server for i5/OS Information Center at:

http://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/index.jsp

To install WebSphere Application Server from the downloaded eimages, follow the instructions in the Information Center documentation (**Installation → Run the GUI Installation tool)**. Instead of placing a physical CD in the CD-ROM drive of your workstation, start the WebSphere Application Server installation by double-clicking the **install.exe** file in the WebSphere Application Server directory that was created when you assembled the eimages as described in 2.3.1, “Assembling the WebSphere Application Server product” on page 20. See Figure 2-19.

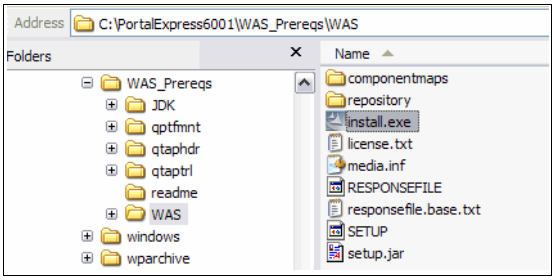


Figure 2-19 Starting the WebSphere Application Server installation

After installing WebSphere Application Server, change the runtime usage limit by running the following i5/OS CL commands:

```
CHGLICINF PRDID(5733W60) FEATURE(5102) USGLMT(*NOMAX)
CHGLICINF PRDID(5733W60) FEATURE(5103) USGLMT(*NOMAX)
```

2.7.1 Installing the WebSphere Application Server PTF group

We recommend that you order the latest PTF group for WebSphere Application Server from IBM before installing the WebSphere Portal Express code, instead of using the PTF group shipped with the WebSphere Portal Express V6 for i5/OS eAssembly package. If you prefer to use the PTF group included in the eAssembly, see the instructions in the instruct.txt file in the readme subdirectory. Figure 2-20 shows the location of the instructions file after assembling the WebSphere Application Server PTF group eimages for V5R4.

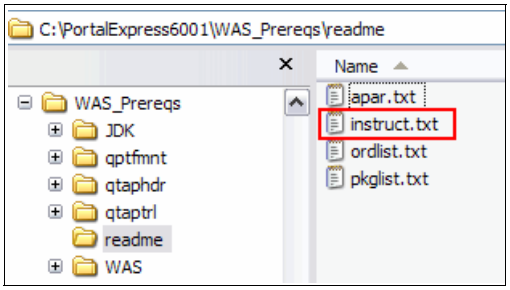


Figure 2-20 WebSphere Application Server 6.0.2.15 installation instructions

If you install the WebSphere Application Server PTF group (the latest one ordered from IBM or the one shipped in the WebSphere Portal Express V6 eAssembly package), you *must* run the **UPDATE** script to complete the fix pack installation after installing the PTF group. The

instructions are located in the readme file on the system. The location of the readme files for WebSphere Application Server V6 is in the following i5/OS integrated file system directory:

```
/QIBM/ProdData/WebSphere/AppServer/V6/Base/updateinstaller/Readme.txt
```

For WebSphere Application Server Network Deployment V6, the location is:

```
/QIBM/ProdData/WebSphere/AppServer/V6/ND/updateinstaller/Readme.txt
```

You can also follow the instructions located in the following URL to complete the installation of the fix pack:

http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver/services/fixpack60.html

2.7.2 Verifying the WebSphere Application Server environment

Perform the following steps to verify the WebSphere Application Server installation:

1. Sign on to a 5250 emulation session.
2. Start the QWAS6 subsystem:

   ```
   STRSBS SBSD(QWAS6/QWAS6)
   ```

3. Enter the Start QSH (STRQSH) CL command on a command line and press Enter.
4. Run the WebSphere Application Server installation verification tool (ivt script):

   ```
   /QIBM/ProdData/WebSphere/AppServer/V6/base/bin/ivt server1 default
   ```

5. Look for the following successful completion messages:

   ```
   IVTL0070I: IVT Verification Succeeded
   IVTL0080I: Installation Verification is complete
   ```

   If the verification is unsuccessful, fix the problems before you proceed.

6. Run the following commands to check the prerequisites:

   ```
   cd /QIBM/ProdData/WebSphere/AppServer/V6/base/bin/
   checkprereqs
   ```

   Look for any messages about a missing PTF or QCCSID value that is not set correctly messages. The following messages show problems in the environment:

   ```
   CFGV7902I:   Warnings:
   PRQV1013W:   Required PTF group SF99114 not applied.
   PRQV1103W:   65535 not recommended for system value QCCSID.
   ```

   The following messages show a successful verification of the prerequisites:

   ```
   CFGV7900I: Summary:
   CFGV7901I:   Informational:
   PRQV1003I:     Optional product 5769LNT option 0000 not installed.
   PRQV1003I:     Optional product 5733LD6 option 0000 not installed.
   ```

7. Verify the successful installation of the WebSphere Application Server fix pack:

   a. From an i5/OS command line, enter the following command by replacing *edition* with `Base` or `ND` and 6.0.2-WS-WAS-OS400PPC64-FPfull0015.install with the fix pack number installed on your system:

      ```
      edtf
      '/QIBM/ProdData/WebSphere/AppServer/V6/<edition>/logs/update/6.0.2-WS-WAS-OS
      400PPC64-FPfull0015.install/updatelog.txt'
      ```

   b. Look for the fix pack successful installation message: `INSTCONFSUCCESS`.

c. Switch to the QSHELL environment by entering the command STRQSH.

d. At the QSH Command Entry, enter the following commands:

```
cd /QIBM/ProdData/WebSphere/AppServer/V6/base/bin
versioninfo
```

e. You see results similar to the ones shown in Figure 2-21.

```
versioninfo
WVER0010I: Copyright (c) IBM Corporation 2002, 2005; All rights reserved.
WVER0011I: WebSphere Application Server Release 6.0
WVER0012I: VersionInfo reporter version 1.15.3.1, dated 4/25/05
--------------------------------------------------------------------------------
IBM WebSphere Application Server Product Installation Status Report
--------------------------------------------------------------------------------
Report at date and time 2007-03-22 12:26:53-0500

Installation
--------------------------------------------------------------------------------
Product Directory /QIBM/ProdData/WebSphere/AppServer/V6/Base
Version Directory /QIBM/ProdData/WebSphere/AppServer/V6/Base/properties/version
DTD Directory     /QIBM/ProdData/WebSphere/AppServer/V6/Base/properties/version/dtd
Log Directory     /QIBM/ProdData/WebSphere/AppServer/V6/Base/logs
Backup Directory  /QIBM/ProdData/WebSphere/AppServer/V6/Base/properties/version/update/backup
TMP Directory     /tmp
Installation Platform
 ------------------------------------------------------------
 Name                      IBM WebSphere Application Server
 Version                   6.0

 Product List
 ------------------------------------------------------------
 BASE                      installed

 Installed Product
 ------------------------------------------------------------
Name                      IBM WebSphere Application Server
Version                   6.0.2.15
ID                        BASE
Build Level               cf150636.04
Build Date                9/5/06

------------------------------------------------------------
End Installation Status Report
------------------------------------------------------------
```

Figure 2-21 Verifying WebSphere Application Server fix pack 15 or later

f. From the same QSHELL Command Entry, enter `historyinfo` and press Enter. Verify that the Maintenance Package ID is 6.0.2-WS-WAS-OS400PPC64-FPfull0015 (or later) for all components.

2.7.3 Installing interim fix after installing WebSphere Application Server fix pack 19

After installing fix pack 19 for IBM WebSphere Application Server V6.0.2, clients running with a non-U.S. Locale Set cannot save configuration changes made to the WebSphere Application Server Administrative Console. You cannot save all changes done inside the WebSphere Administrator Console, and a message similar to the one shown in Figure 2-22 is displayed.

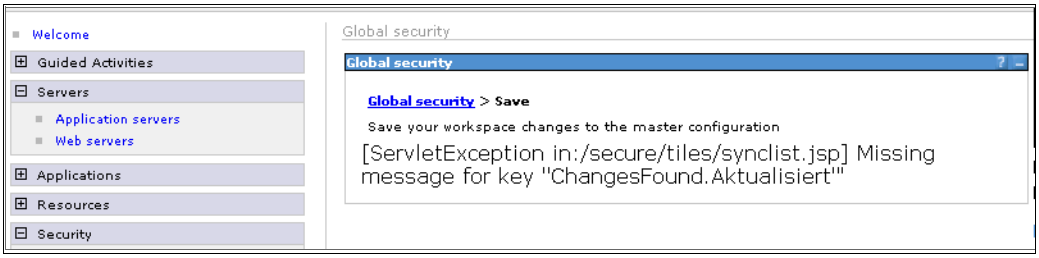


Figure 2-22 Error message when trying to save changes

This problem happens for all WebSphere Application Server platforms.

An interim fix PK44764 addresses this problem. You can download it from the following Web site:

http://www.ibm.com/support/docview.wss?rs=180&uid=swg24015914

The fix for this APAR is currently targeted for inclusion in fix pack 6.0.2.21.

Installation instructions for interim fix PK44764 are:

1. Download Fix Pack PK44764 from the previously listed Web site to your workstation.
2. Copy the file to the following i5/OS integrated file system directory:

   `/QIBM/ProdData/WebSphere/AppServer/V6/Base/updateinstaller/maintenance`
3. Stop all WebSphere Application Server profiles and end the subsystem QWAS6 (`ENDSBS QWAS6 *immed`).
4. Start a QShell session from an i5/OC command line with `STRQSH`.
5. Change to the updateinstaller directory:

   `cd /QIBM/ProdData/websphere/appserver/v6/base/updateinstaller`
6. Call the update installer by typing `update` and press Enter.
7. You see messages. The installation of the fix is done when the job ends.
8. Review the updatelog.txt file, which is located in the following directory:

   `/QIBM/ProdData/WebSphere/AppServer/V6/<edition>/logs/update/6.0.2.19-WS-WAS-IFPK44764`
9. Start the WebSphere Application profiles.

2.8 Preparing the IBM Directory Server for i5/OS

WebSphere Portal Express uses Lightweight Directory Access Protocol (LDAP) to store user information for authentication purposes. This section describes the minimum preparation required for IBM Directory Services included with i5/OS before configuring a WebSphere

Portal Express profile using the Create Portal for i5/OS wizard. For more advanced LDAP configuration scenarios with WebSphere Portal Express, see the IBM Redpaper *Enabling Collaboration in WebSphere Portal Express V6 on i5/OS*, REDP-4310.

2.8.1 Supported LDAP directories

You can use the following LDAP directories to secure WebSphere Portal Express V6:

- IBM Tivoli® Directory Server V6.0
- IBM Tivoli Directory Server V5.2
- IBM Tivoli Directory Server V5.1
- IBM Lotus Domino 7.0.1
- IBM Lotus Domino 6.5.5
- IBM Lotus Domino 6.5.4
- Novell eDirectory V8.7.3
- Sun™ Java™ System Directory Server V5.2
- Microsoft Active Directory® 2003
- Microsoft Active Directory 2000
- Microsoft Active Directory Application Mode (ADAM) 2003

Note: The i5/OS V5R4 Directory Server is equivalent to the IBM Tivoli Directory Server V5.2. The i5/OS V5R3 Directory Server is equivalent to the IBM Tivoli Directory Server V5.1.

When using the Create WebSphere Portal wizard in IBM Web Administration for i5/OS to configure a WebSphere Portal Express server, the Microsoft Active Directory Application Mode (ADAM) 2003 is not supported.

2.8.2 Terminology

This section provides a quick reference as you review your directory server's configuration:

- *Suffix*: This is the top entry in your LDAP directory information tree. This is also referred to as the *base entry* or the *root*. There are several suffixes in an LDAP directory, each representing the top of a separate directory information tree.
- *Default suffix*: This is the LDAP suffix that exists in the Directory Server by default. It has a format of `DC=system,DC=subdomain1,DC=subdomain2`. For example, if the System i host name is `itcebiz1.rchland.ibm.com`, the default suffix is `DC=itcebiz1,DC=rchland,DC=ibm.com`.
- *Users container*: This is the container in the LDAP directory where information about WebSphere Portal Express users is stored.
- *Groups container*: This is the container in the LDAP directory where information about WebSphere Portal Express groups is stored.
- *LDAP administrator*: This is the user account in the directory server that has read/write authority to the directory server.
- *Distinguished names*: Every entry in the directory has a distinguished name (DN). The DN is the name that uniquely identifies an entry in the directory. A DN is made up of attribute=value pairs separated by commas, for example: `DC=itcebiz1,DC=rchland,DC=ibm.com`
- *User Parent DN*: This specifies the user parent DN for the LDAP server, for example: `cn=users,DC=system,DC=subdomain1,DC=subdomain2`

- *Group Parent DN*: This specifies the group parent DN for the LDAP server, for example: `cn=groups,DC=system,DC=subdomain1,DC=subdomain2`

The portal administrator user resides in your LDAP directory in a user container, and the portal administrator group resides in a group container. When you configure LDAP using the Create WebSphere Portal wizard for i5/OS, you must specify the User Parent DN and Group Parent DN where the portal administrator user and portal administrator group will reside.

For additional information about LDAP, see *Implementation and Practical Use of LDAP on the IBM eServer iSeries Server*, SG24-6193, at:

`http://www.redbooks.ibm.com/abstracts/sg246193.html`

2.8.3 Using the default LDAP suffix

If you use the default LDAP suffix, you need to do little besides checking that your LDAP server is working properly. As described in 2.8.2, "Terminology" on page 40, you are using the default LDAP suffix if the suffix is of the format `DC=system,DC=subdomain1,DC=subdomain2`. This suffix is created by default.

Perform the following steps to verify the basic setup of your LDAP directory:

1. Start the iSeries Navigator and expand ***your system*** → **Network** → **Servers** → **TCP/IP**.
2. Right-click **IBM Directory Server** and select **Properties** (Figure 2-23).

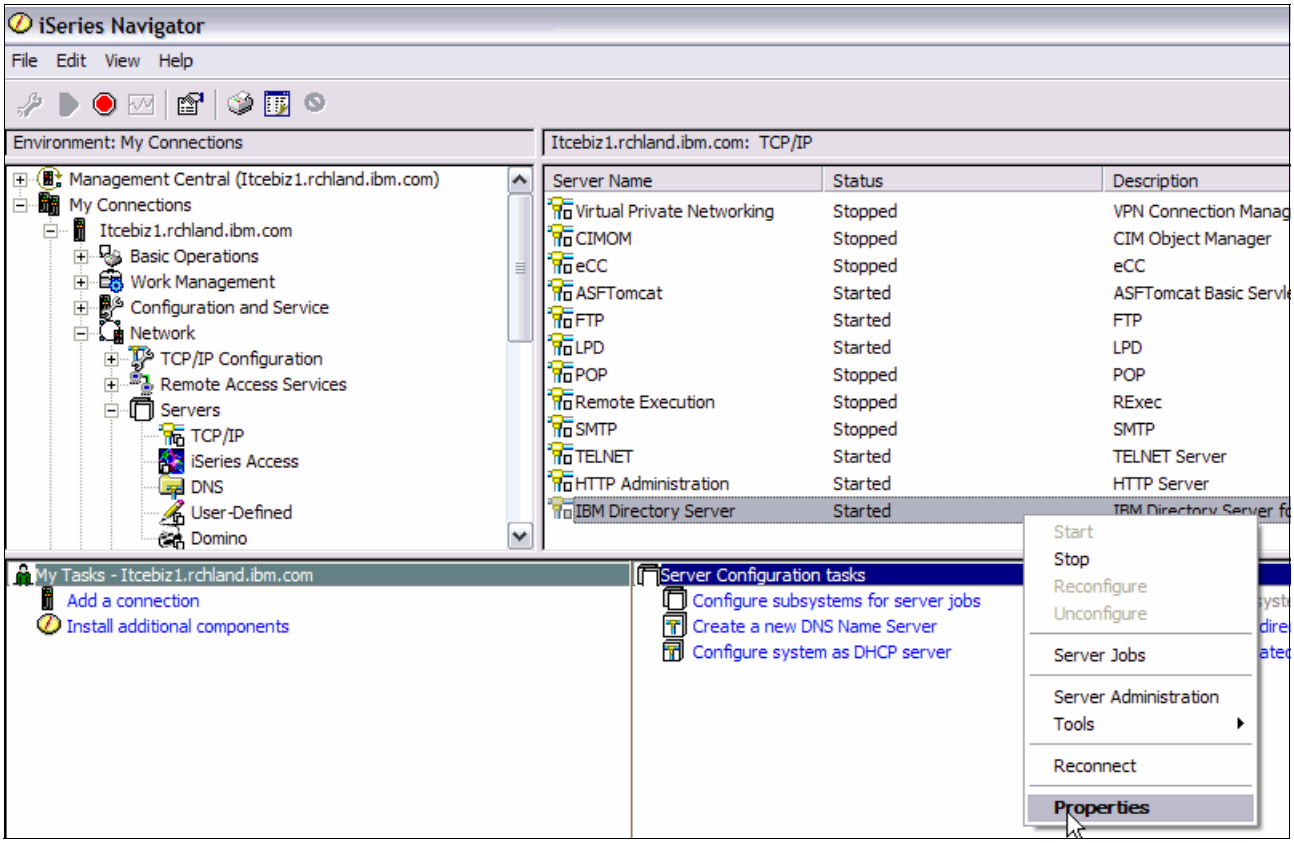


Figure 2-23 Selecting IBM Directory Server properties

3. On the IBM Directory Server Properties window, click the **Database/Suffixes** tab and verify there is a suffix of `DC=system,DC=subdomain1,DC=subdomain2`. For example, for a host name of `itcebiz1.rchland.ibm.com`, the default suffix is `DC=itcebiz1,DC=rchland,DC=ibm.com` (see Figure 2-24).

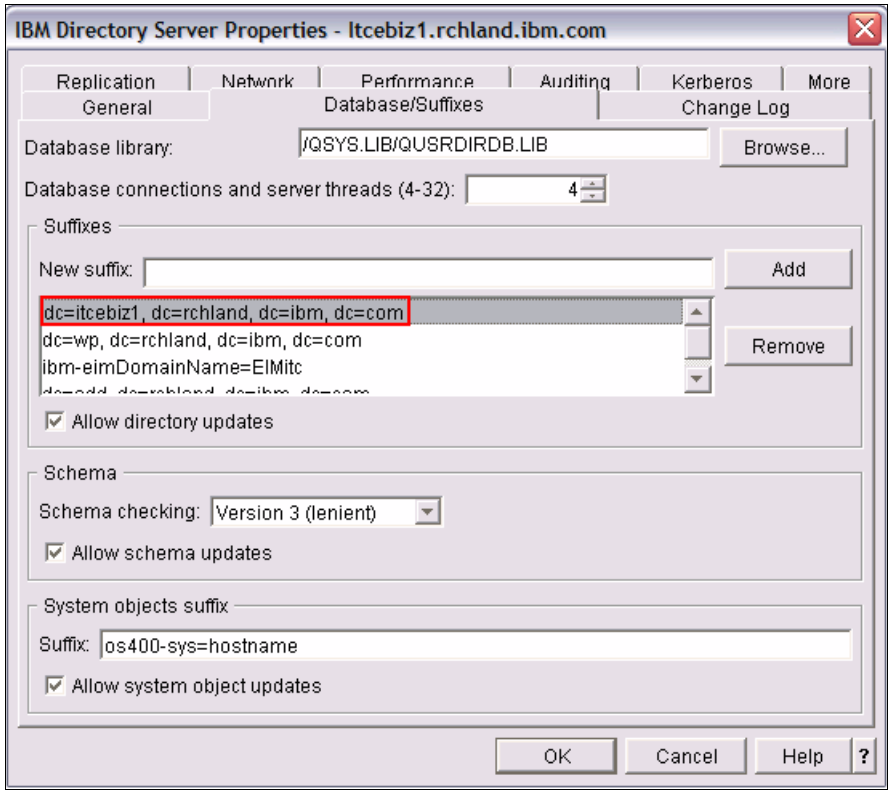


Figure 2-24 Verifying the default LDAP suffix

4. If you do not know the password for the LDAP administrator or want to reset the password, perform the following steps (Figure 2-25):
   a. Click the **General** tab.
   b. Click **Password**.
   c. Enter the password twice and click **OK**.
   d. Restart the directory server.

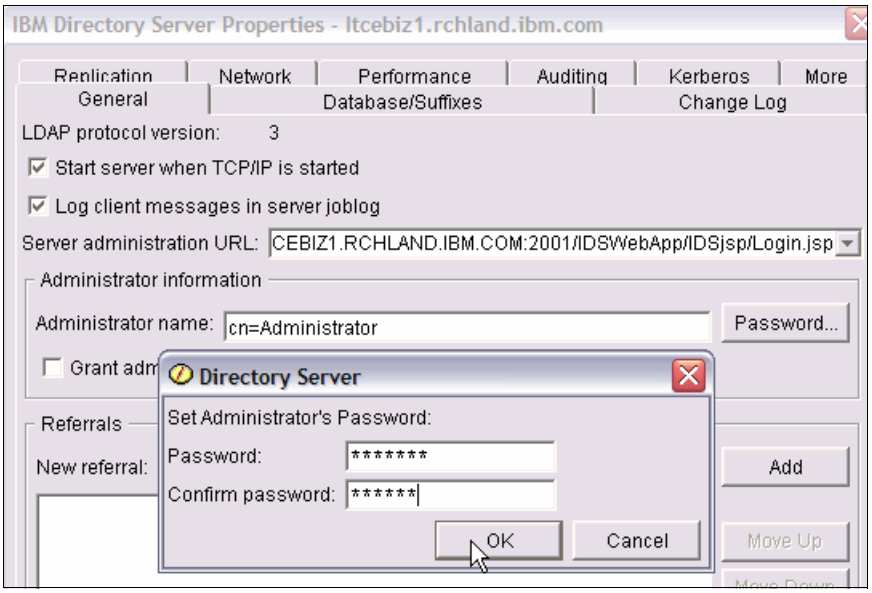


Figure 2-25 Changing the LDAP administrator password

2.8.4 Creating a new LDAP suffix

You might need to separate LDAP environments, such as production and test environments. Creating a separate LDAP suffix allows you to separate the environments. Multiple WebSphere Portal Express profiles can run on the same System i machine, sharing the same LDAP suffix or using individual suffixes.

To add a new LDAP suffix to the LDAP directory, perform the following steps:

1. From iSeries Navigator, expand ***your system*** → **Network** → **Servers** → **TCP/IP**.
2. Right-click **IBM Directory Server** and select **Properties** (Figure 2-23 on page 41).
3. Select the **Database/Suffixes** tab.
4. In the New suffix field, type the new suffix, for example, `dc=mysuffix, dc=test, dc=com`, and click **Add**. Click **OK** (Figure 2-26 on page 44).

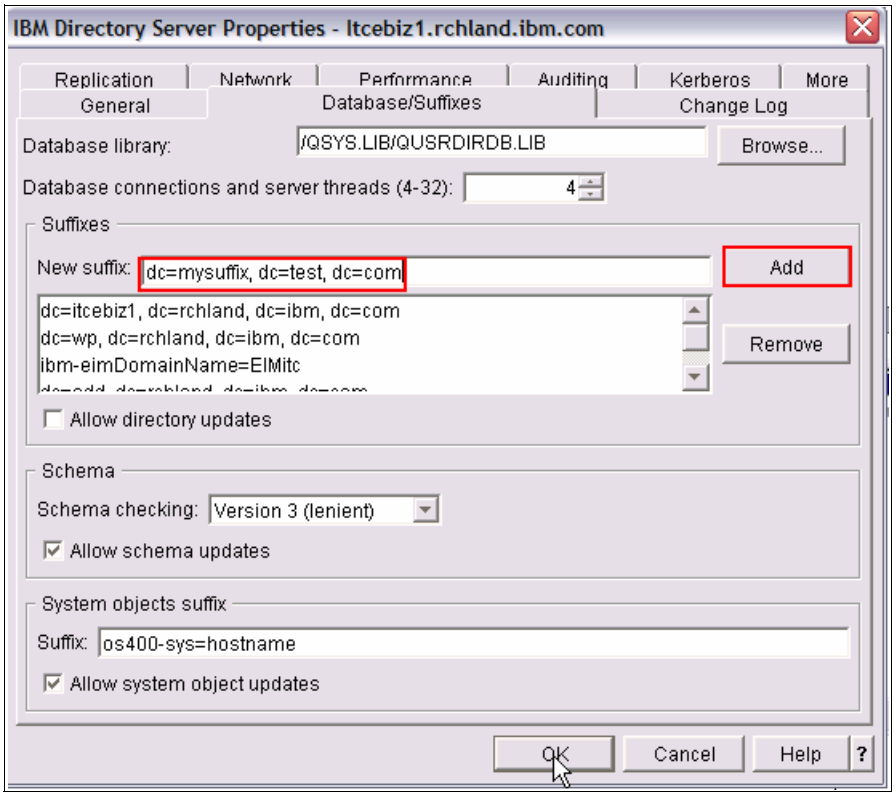


Figure 2-26 Adding a new LDAP suffix

Adding the users and groups containers

If you use an LDAP suffix other than the default suffix, the Create WebSphere Portal for i5/OS wizard does not create the *users* and *groups* containers, even if you allow write access to the directory. To create the users and groups containers, perform the following steps:

1. Copy the PortalUsers.ldif file from the setup CD (or C97Q3ML eimage) to c:\temp on your local PC drive.
2. Edit the PortalUsers.ldif file using WordPad or another text file editor.
3. Remove all the entries starting with `dn: uid=wpsadmin,cn=users,dc=yourco,dc=com` to the end of the file.
4. Replace all instances of `dc=yourco,dc=com` with your suffix DN. For example: `dc=mysuffix, dc=test, dc=com`.
5. The PortalUsers.ldif file looks similar to the one shown in Figure 2-27 on page 45.

```
version: 1

# NOTE: you must edit this file before importing it and replace all
# occurrences of the default suffix "dc=yourco,dc=com" with the suffix
# that your LDAP server is configured for.

dn: dc=mysuffix,dc=test,dc=com
objectclass: domain
objectclass: top
# Add lines according to this scheme that correspond to your suffix
dc: dc=mysuffix,dc=test,dc=com
dc: mysuffix

dn: cn=users,dc=mysuffix,dc=test,dc=com
objectclass: container
objectclass: top
cn: users

dn: cn=groups,dc=mysuffix,dc=test,dc=com
objectclass: top
objectclass: container
cn: groups
```

Figure 2-27 PortalUsers.ldif file modified to create the users and groups containers

6. Save and close the PortalUsers.ldif file. Verify that `txt` has not been added to the file extension.
7. Copy the modified PortalUsers.ldif file to an i5/OS integrated file system directory on your system.
8. Stop the IBM Directory Server:
   a. From the iSeries Navigator, click **Network** → **Servers** → **TCP/IP**.
   b. Right-click IBM Directory and select **Server** → **Stop**.
9. Import the PortalUsers.ldif file:
   a. From the iSeries Navigator, right-click **IBM Directory Server** and select **Tools** → **Import File**.
   b. Click **Browse** and select the i5/OS integrated file system directory where you copied the PortalUsers.ldif file.
   c. Click **OK** twice (Figure 2-28).

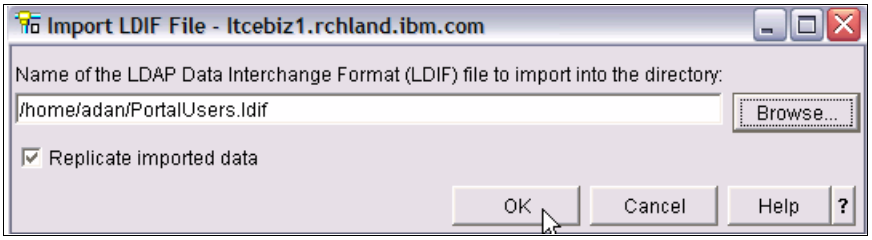


Figure 2-28 Importing the PortalUsers.ldif file

10. When the import operation is complete, click **Done**.

11. Start the IBM Directory Server:
    a. From the iSeries Navigator, click **Network** → **Servers** → **TCP/IP**.
    b. Right-click I**BM Directory Server** and select **Start**.

2.9 Supported Web browsers

The following Web browsers are supported:

- Microsoft Internet Explorer® V6.0 SP2
- Firefox V1.5.0.3

The Web browsers were tested on servers that support the following client operating systems or desktop products:

- Desktop Linux Distributions
- Microsoft Windows 2000 SP4
- Microsoft Windows XP SP2
- Apple Mac OS X

3

Installing and configuring WebSphere Portal Express

This chapter provides step-by-step instructions on installing WebSphere Portal Express from electronic images. It outlines the recommended path to get your first WebSphere Portal Express environment up and running on your System i machine quickly.

This chapter discusses the following topics:

- "Installing WebSphere Portal Express from electronic images" on page 48
- "Configuring WebSphere Portal Express with IBM Web Administration for i5/OS" on page 71
- "Understanding WebSphere Portal Express work management on i5/OS" on page 90
- "Problem determination" on page 96
- "Deleting a WebSphere Portal Express profile" on page 101
- "Uninstalling the WebSphere Portal Express product" on page 103

WebSphere Portal Express provides many installation and configuration options not discussed in this Redpaper. This Redpaper helps you get started quickly with a simple deployment example. For information about other planning considerations and topologies, see the WebSphere Portal Version 6 Information Center at:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp

© Copyright IBM Corp. 2007. All rights reserved.

3.1 Installing WebSphere Portal Express from electronic images

After assembling the eimages as described in 2.3.2, “Assembling WebSphere Portal Express” on page 20, you can proceed to installing WebSphere Portal Express V6 on your System i machine. You must have an i5/OS user profile with *IOSYSCFG, *ALLOBJ, and *JOBCTL special authorities to perform the installation.

Important: Do not use the QSECOFR user profile to perform the WebSphere Portal Express installation.

You can select one of two installation options:

- Install and Configure
- Install only

The easiest way to get WebSphere Portal Express up and running on i5/OS is to select the `Install only` installation option and then configure the portal profile using the IBM Web Administration for i5/OS. If you cannot use IBM Web Administration for i5/OS to configure your portal environment (for example, you want to configure the portal profile on WebSphere Application Server ND), use the Install and Configure option.

Perform the following steps to prepare for the installation of WebSphere Portal Express:

1. Start the following subsystems by issuing the following Start Subsystem (STRSBS) CL commands:
   - `STRSBS SBSD(QSYSWRK)`
   - `STRSBS SBSD(QUSRWRK)`
   - `STRSBS SBSD(QSERVER)`
   - `STRSBS SBSD(QWAS6/QWAS6)`
2. Start the host servers by issuing the `STRHOSTSVR SERVER(*ALL)` command.
3. Make sure that you can successfully ping the host name of your System i machine from the PC you are using to install WebSphere Portal Express.
4. Stop any personal firewalls on your PC client.
5. Telnet from the PC client to System i and from System i to the PC client (the last Telnet will fail, but this test is useful in networks that require authentication via internal firewalls).
6. Do not use a remote desktop to perform a portal installation.
7. Proceed with the WebSphere Portal Express installation. Refer to 3.1.1, “Install only option (recommended method)” on page 48 or 3.1.2, “Install and configure option” on page 59.

3.1.1 Install only option (recommended method)

Perform the following steps to perform the install only option:

1. From Windows Explorer, change to the directory where you assembled the WebSphere Portal Express product image.

2. Double-click the launchpad, the **setup.exe** file (Figure 3-1).

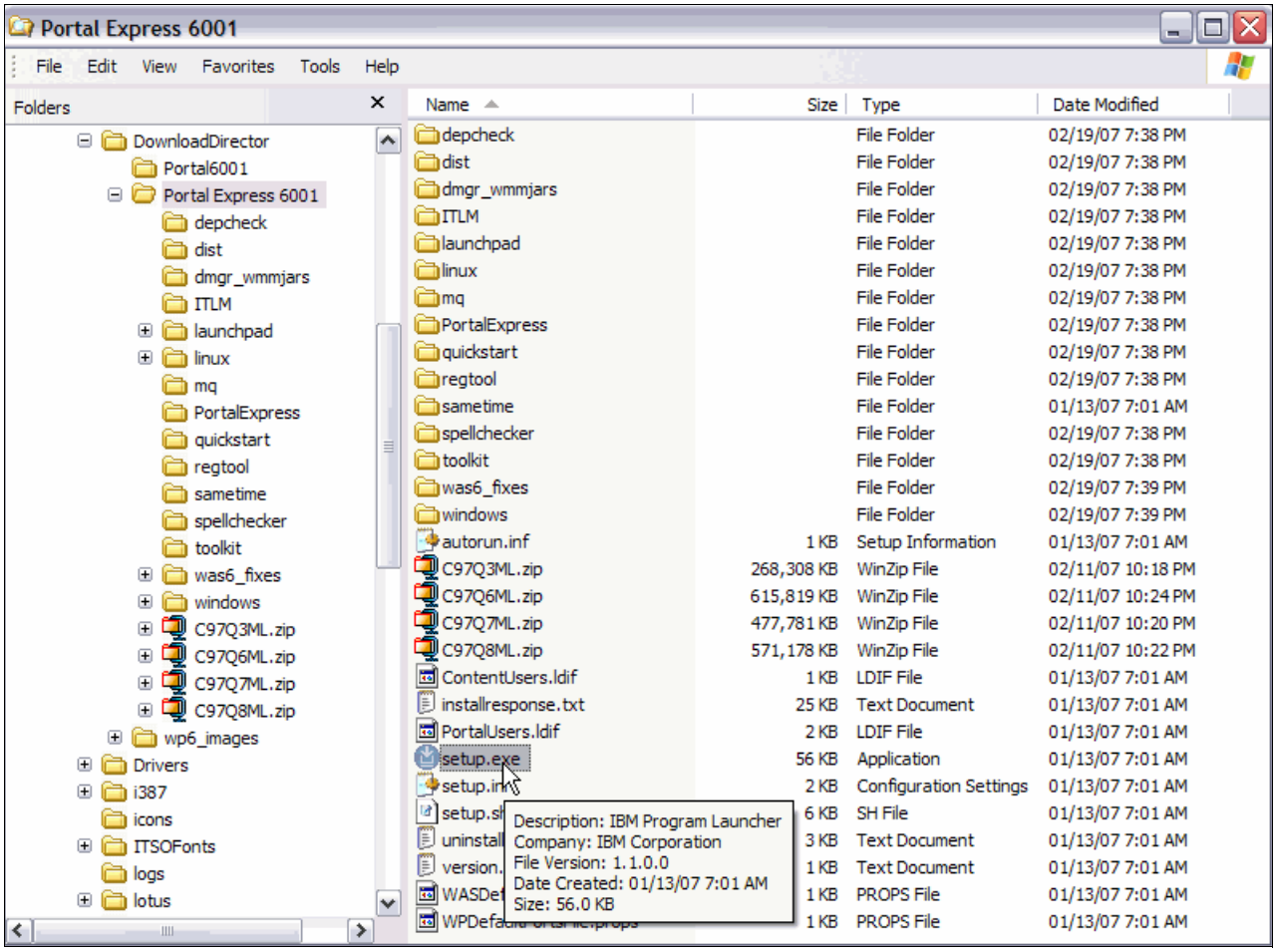


Figure 3-1 Launching the portal installation

3. The WebSphere Portal Express launchpad includes links to useful information to get you started, such as the Quick Start Guide, prerequisite hardware and software, and product documentation. Notice that you can select the language in the upper right corner of the window. Use the navigation links on the left to view the information in each panel (Figure 3-2). Click **Install**.

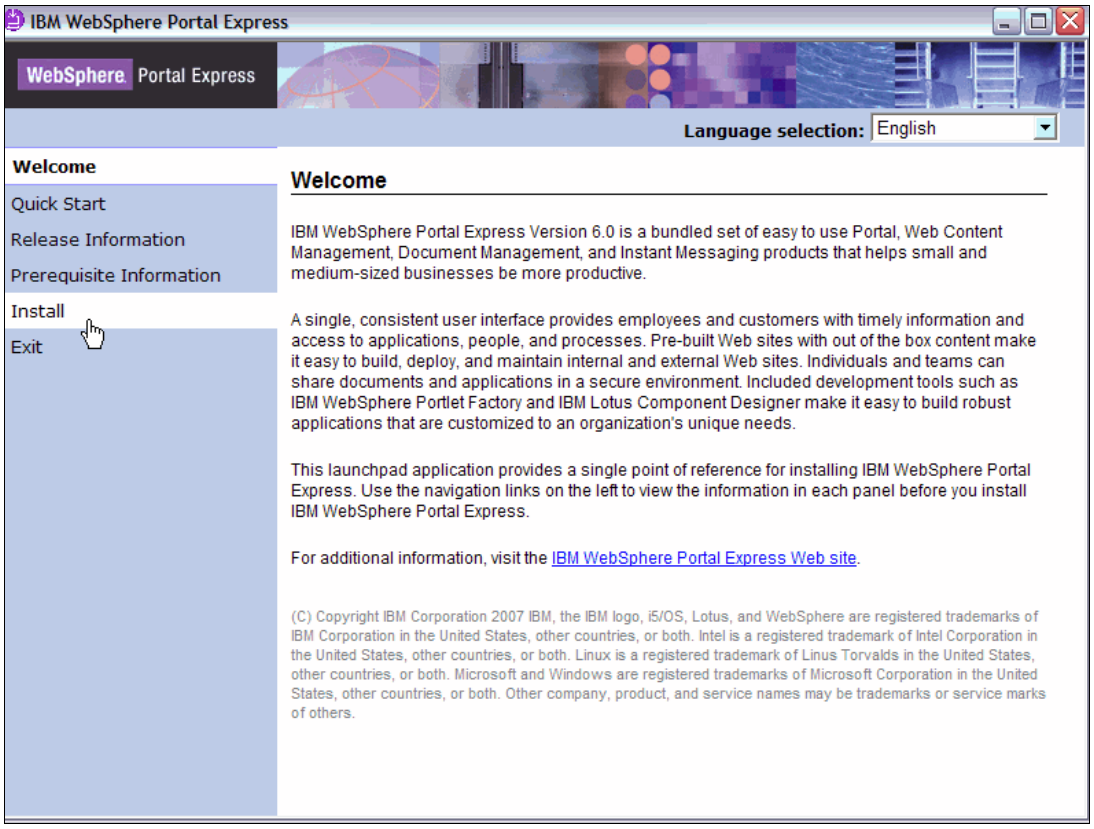

IBM WebSphere Portal Express
WebSphere Portal Express
Language selection: English
Welcome
Quick Start
Release Information
Prerequisite Information
Install
Exit
Welcome
IBM WebSphere Portal Express Version 6.0 is a bundled set of easy to use Portal, Web Content Management, Document Management, and Instant Messaging products that helps small and medium-sized businesses be more productive.
A single, consistent user interface provides employees and customers with timely information and access to applications, people, and processes. Pre-built Web sites with out of the box content make it easy to build, deploy, and maintain internal and external Web sites. Individuals and teams can share documents and applications in a secure environment. Included development tools such as IBM WebSphere Portlet Factory and IBM Lotus Component Designer make it easy to build robust applications that are customized to an organization's unique needs.
This launchpad application provides a single point of reference for installing IBM WebSphere Portal Express. Use the navigation links on the left to view the information in each panel before you install IBM WebSphere Portal Express.
For additional information, visit the IBM WebSphere Portal Express Web site.
(C) Copyright IBM Corporation 2007 IBM, the IBM logo, i5/OS, Lotus, and WebSphere are registered trademarks of IBM Corporation in the United States, other countries, or both. Intel is a registered trademark of Intel Corporation in the United States, other countries, or both. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both. Other company, product, and service names may be trademarks or service marks of others.

Figure 3-2 WebSphere Portal Express launchpad

4. On the Install IBM WebSphere Portal Express window, select **Launch the installation wizard for i5/OS** (Figure 3-3).

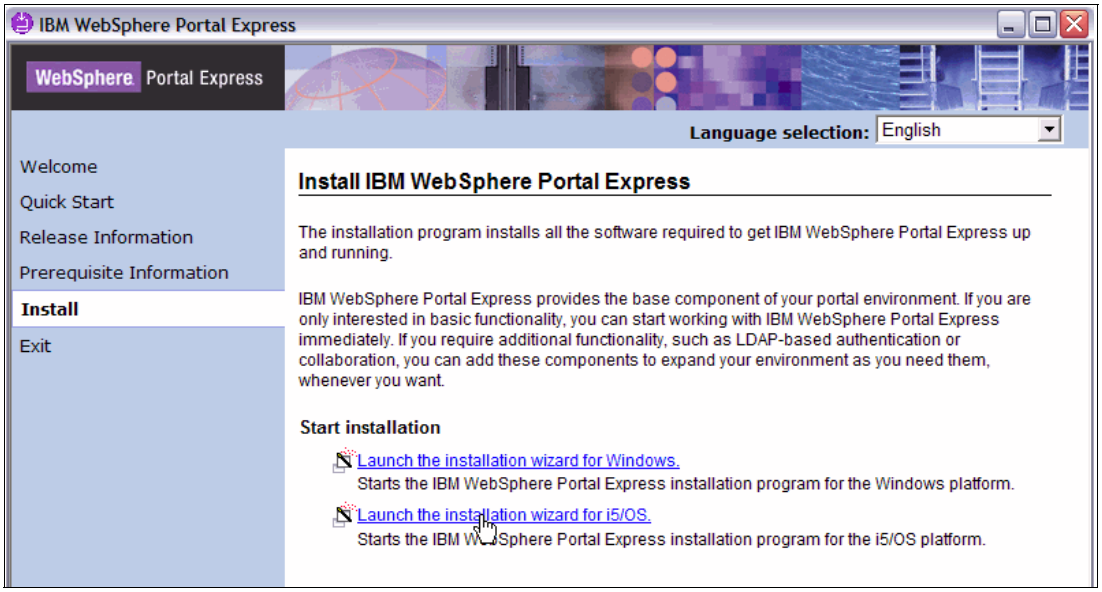

IBM WebSphere Portal Express
WebSphere Portal Express
Language selection: English
Welcome
Quick Start
Release Information
Prerequisite Information
Install
Exit
Install IBM WebSphere Portal Express
The installation program installs all the software required to get IBM WebSphere Portal Express up and running.
IBM WebSphere Portal Express provides the base component of your portal environment. If you are only interested in basic functionality, you can start working with IBM WebSphere Portal Express immediately. If you require additional functionality, such as LDAP-based authentication or collaboration, you can add these components to expand your environment as you need them, whenever you want.
Start installation
Launch the installation wizard for Windows.
Starts the IBM WebSphere Portal Express installation program for the Windows platform.
Launch the installation wizard for i5/OS.
Starts the IBM WebSphere Portal Express installation program for the i5/OS platform.

Figure 3-3 Launching WebSphere Portal Express installation for i5/OS

5. On the Signon to the Server window (Figure 3-4), enter the following information:
   a. System: Your System i fully qualified host name or IP address.
   b. User ID: An i5/OS user profile with *IOSYSCFG, *JOBCTL, and *ALLOBJ authorities.

      Important: Do not use the QSECOFR user profile.

   c. Password: The user ID's password.
   d. Click **OK**.

      Tip: If you enter the wrong user ID or password, the Signon to the Server window goes away without an error message.

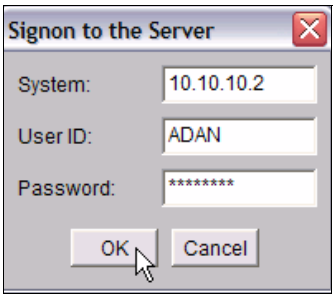


Figure 3-4 Signing on to System i machine

6. On the Installer window (Figure 3-5), select the language for the InstallShield for Multi Platforms (ISMP) program. Click **OK**.

Figure 3-5 Selecting a language for the installation wizard

7. On the WebSphere Portal Express Version 6.0 Installer window (Figure 3-6), click **Next**. The installation wizard then performs prerequisite checking before starting the installation.

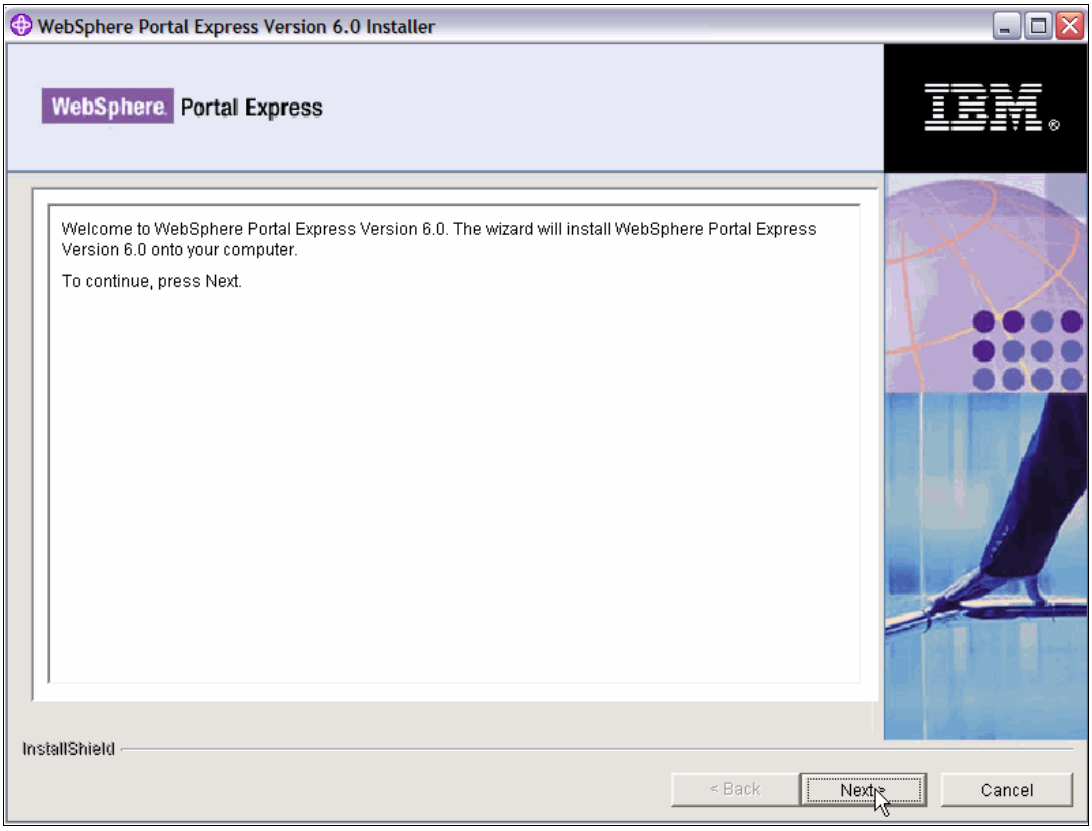

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
Welcome to WebSphere Portal Express Version 6.0. The wizard will install WebSphere Portal Express Version 6.0 onto your computer.
To continue, press Next.
InstallShield
< Back
Next >
Cancel

Figure 3-6 WebSphere Portal Express installer

8. On the Software License Agreement window (Figure 3-7), accept the license terms and click **Next**.

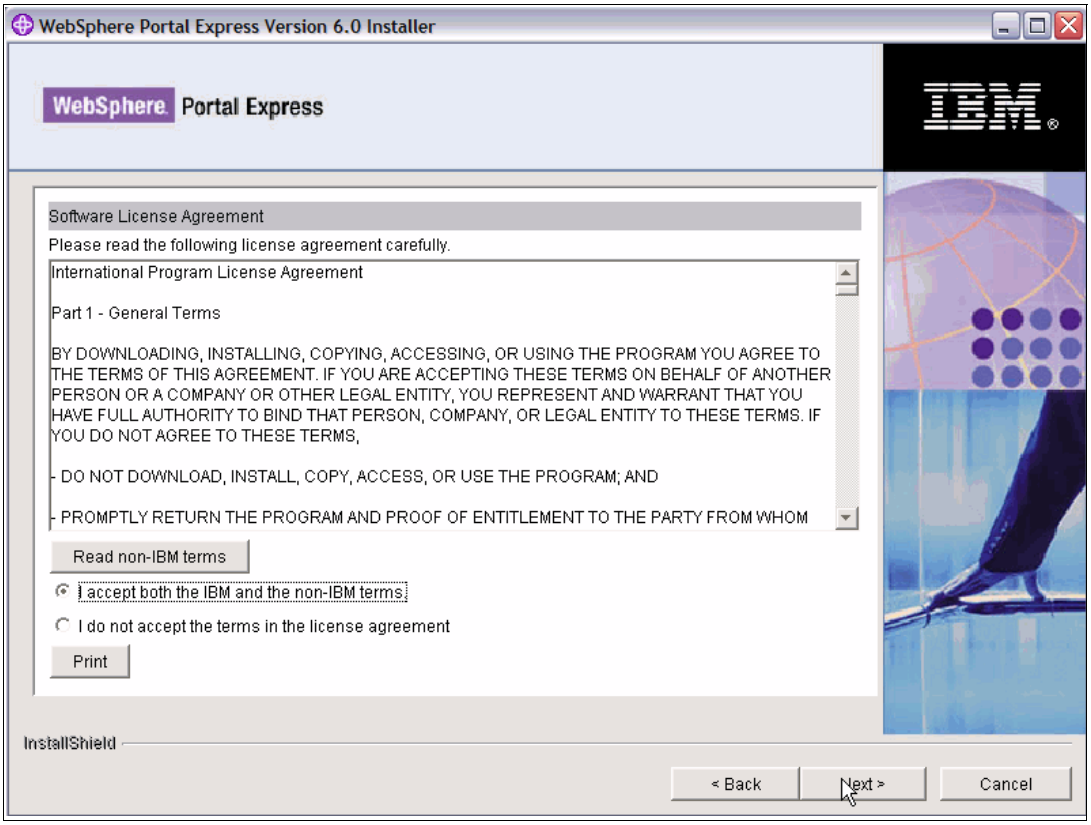

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
Software License Agreement
Please read the following license agreement carefully.
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
- PROMPTLY RETURN THE PROGRAM AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM
Read non-IBM terms
I accept both the IBM and the non-IBM terms
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

Figure 3-7 WebSphere Portal Express software license agreement

9. On the Basic Configuration Option window (Figure 3-8), select the **Install only** option to install the WebSphere Portal Express Version 6 code in the i5/OS integrated file system directory of /QIBM/ProdData/PortalExpress/V6. In this example, we perform the WebSphere Portal Express server configuration later using the IBM Web Administration for i5/OS. Click **Next**.

> **Tip:** The remote installation of the product files can take approximately 15 minutes. At this point, the file /tmp/Installshield/portalinstall.lockfile is created in the i5/OS integrated file system directory, and it is removed after the installation finishes. If a previous attempt to install the product has not finished successfully, you might see an error message now. You need to delete portalinstall.lockfile before you can continue.

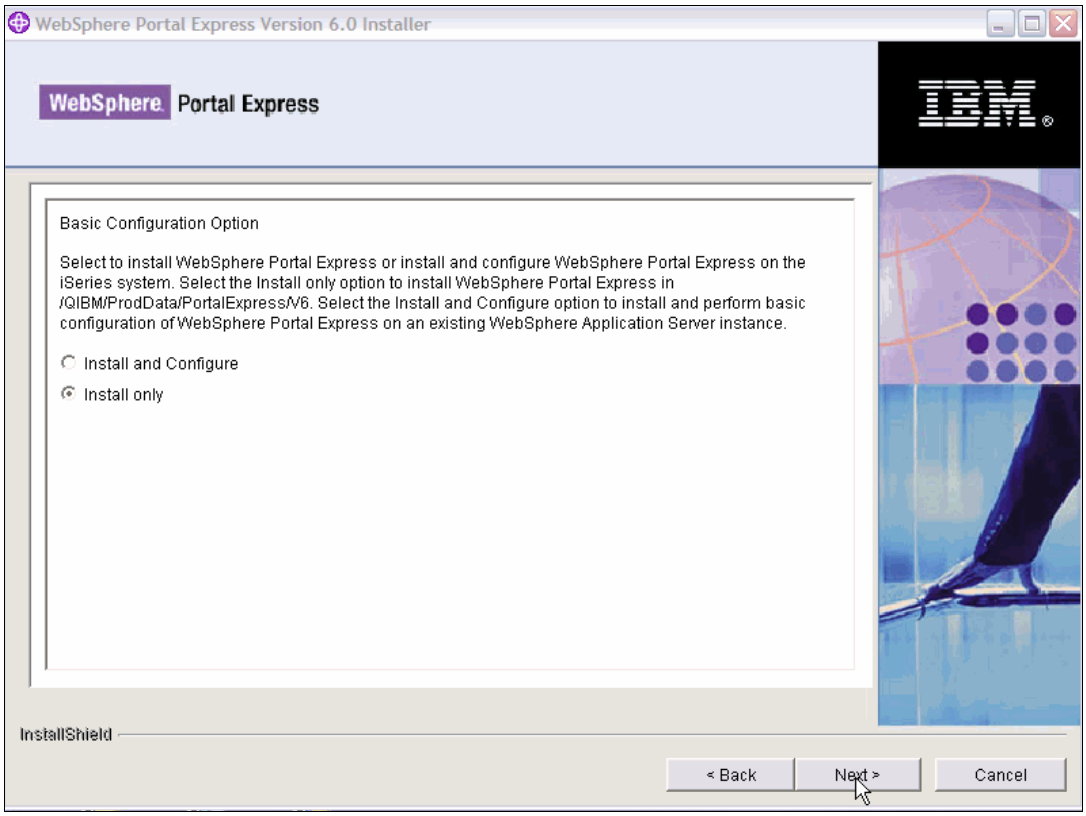

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
Basic Configuration Option
Select to install WebSphere Portal Express or install and configure WebSphere Portal Express on the iSeries system. Select the Install only option to install WebSphere Portal Express in /QIBM/ProdData/PortalExpress/V6. Select the Install and Configure option to install and perform basic configuration of WebSphere Portal Express on an existing WebSphere Application Server instance.
Install and Configure
Install only
InstallShield
< Back
Next >
Cancel

Figure 3-8 WebSphere Portal Express Install only option

10. WebSphere Portal Express is ready to install. Click **Next**. See Figure 3-9.

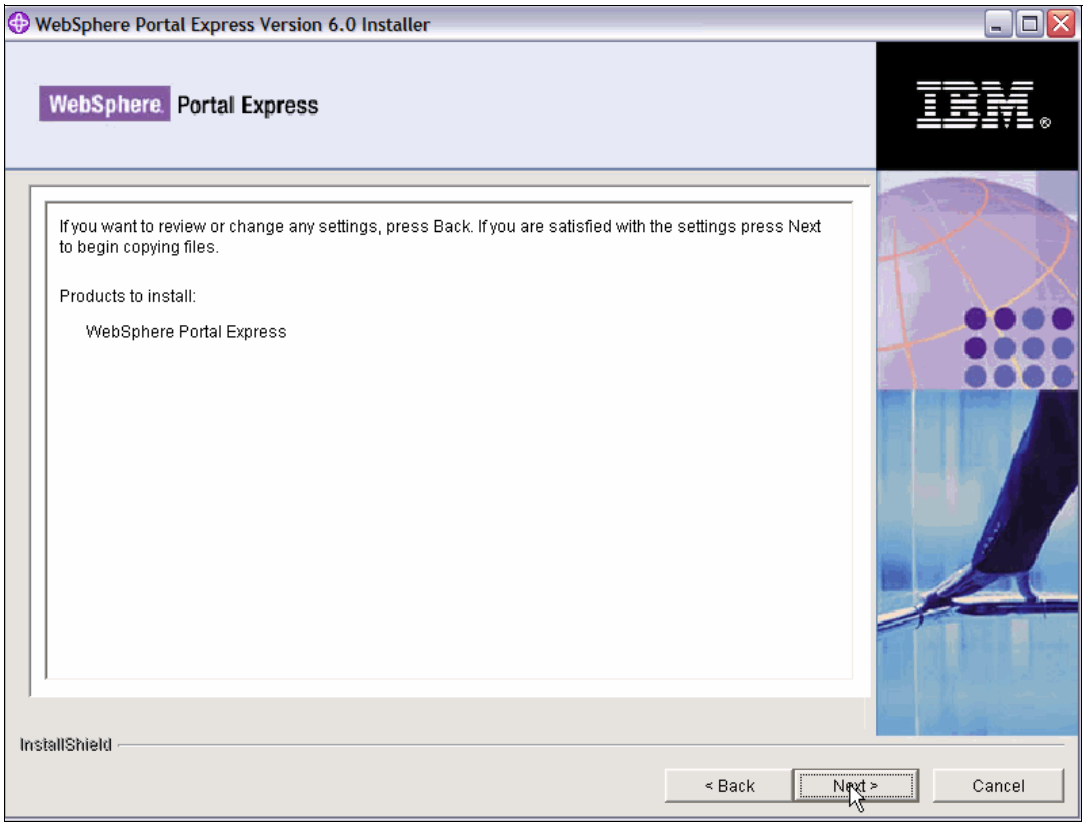

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
If you want to review or change any settings, press Back. If you are satisfied with the settings press Next to begin copying files.
Products to install:
WebSphere Portal Express
InstallShield
< Back
Next >
Cancel

Figure 3-9 WebSphere Portal Express ready to install

11. Notice the location of the installation logs as shown in Figure 3-10.

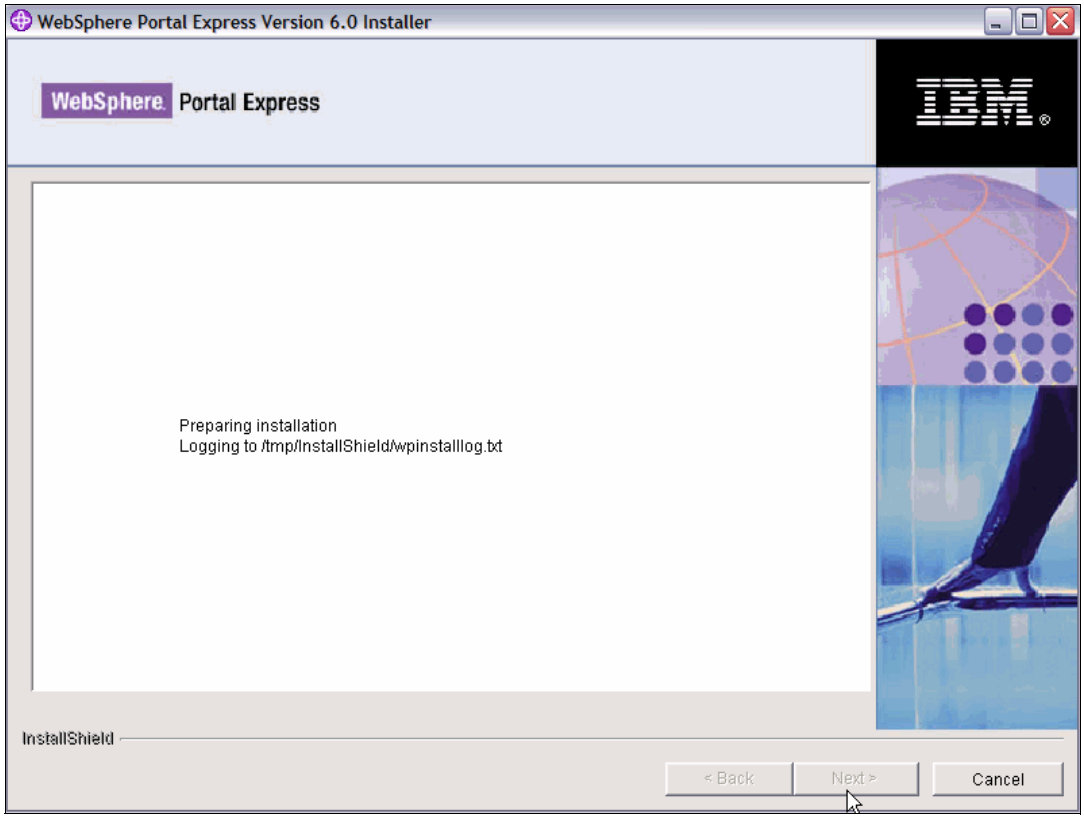


Figure 3-10 WebSphere Portal Express installation log location

12. The installation image files are copied to /QIBM/ProdData/PortalExpress/V6 as shown in Figure 3-11.

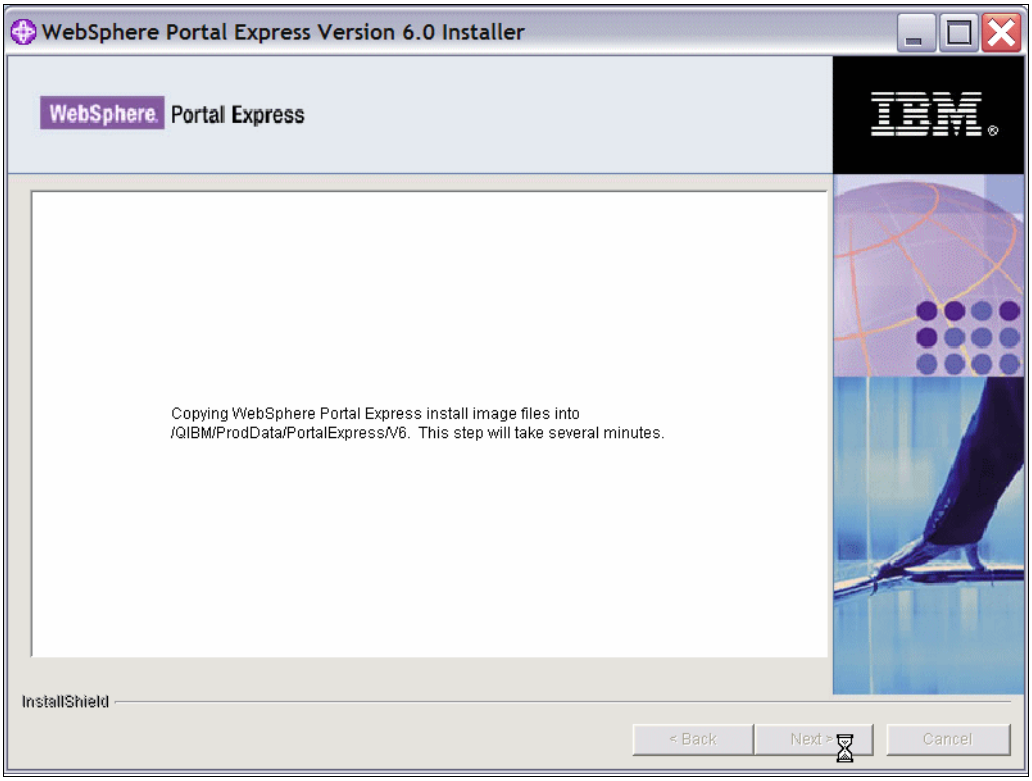


Figure 3-11 Copying the installation image files into /QIBM/ProdData/PortalExpress/V6

13. The progress indicator shown in Figure 3-12 might not move during the copy of the installation images files to the ProdData directory; however, the installation is still in progress. Do not cancel it, just wait.

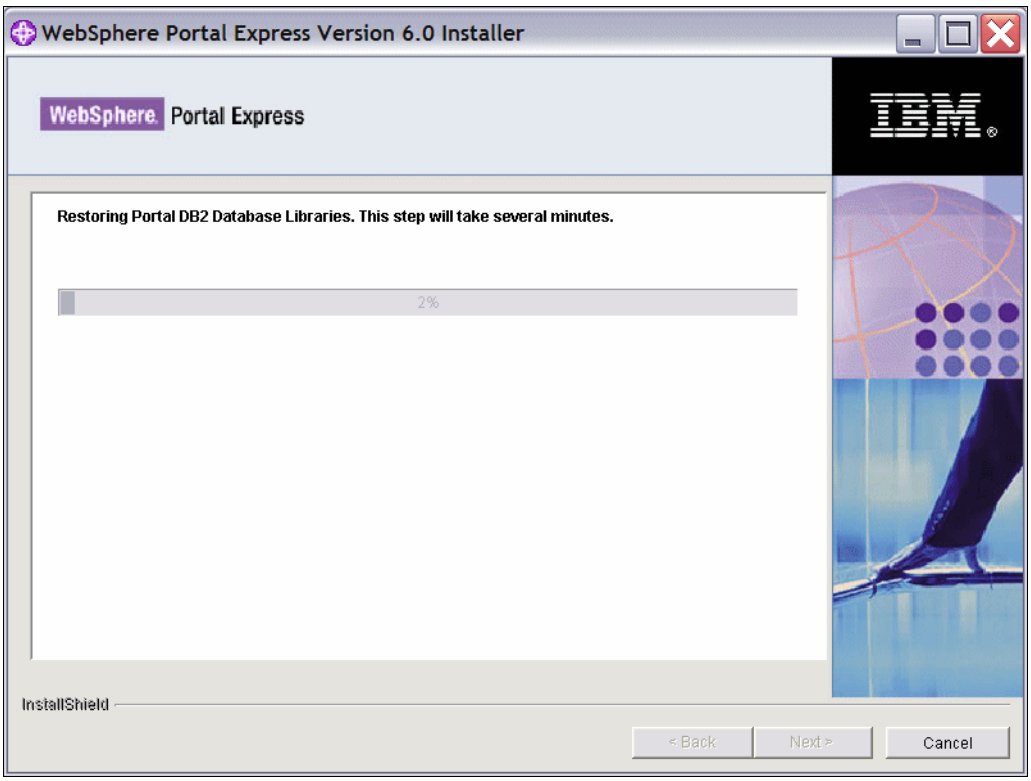


Figure 3-12 Restoring the Portal DB2 database libraries

14. The WebSphere Portal Express product library and databases are restored. At the successful installation message shown in Figure 3-13, take note of the log directory and click **Finish**.

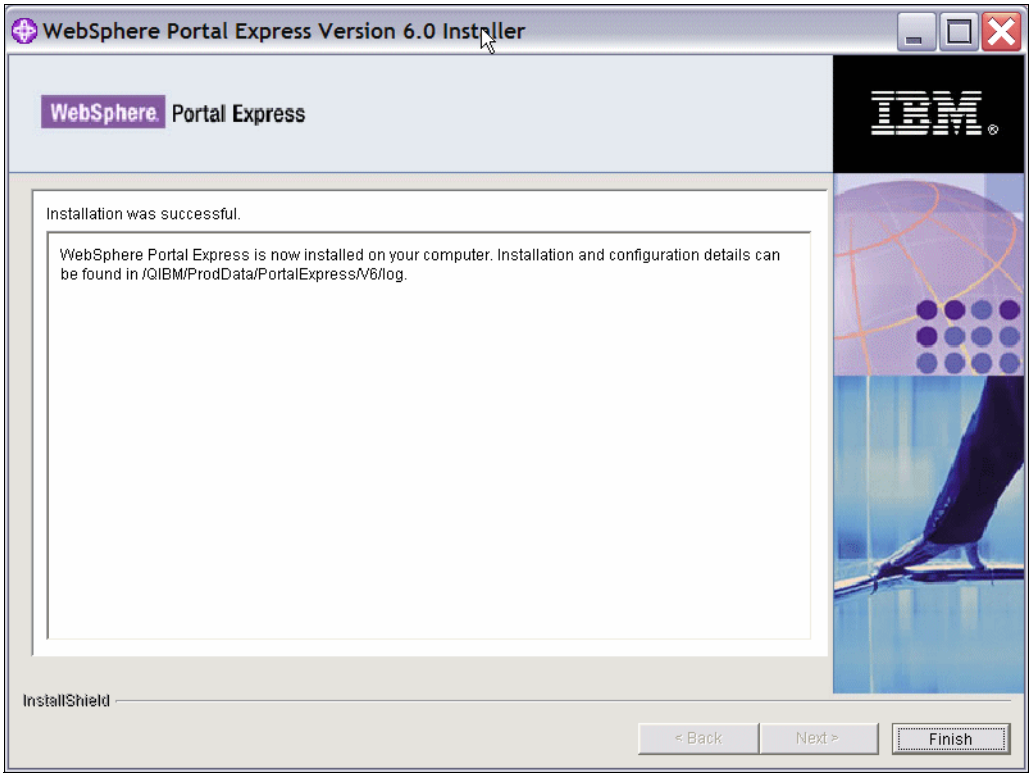

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
Installation was successful.
WebSphere Portal Express is now installed on your computer. Installation and configuration details can be found in /QIBM/ProdData/PortalExpress/V6/log.
InstallShield
< Back
Next >
Finish

Figure 3-13 WebSphere Portal Express successful installation

3.1.2 Install and configure option

You can select the Install and Configure option only for initial product installation and profile configuration. Perform the following steps:

1. Perform Steps 1 on page 48 through Step 8 on page 53 in 3.1.1, “Install only option (recommended method)” on page 48.

2. On the Basic Configuration Option window (Figure 3-14), select **Install and Configure** and click **Next**.

> **Important:** A port number is automatically chosen by the installation program when the profile is created. The starting port is based on a range of 50 free ports within ports 10000 to 65000. The installation attempts to detect port conflicts with servers that are *started* on the system when the installation and configuration option runs. If the installation program cannot detect ports for WebSphere Application Server or WebSphere Portal Express, a warning message states that there was a problem detecting ports.

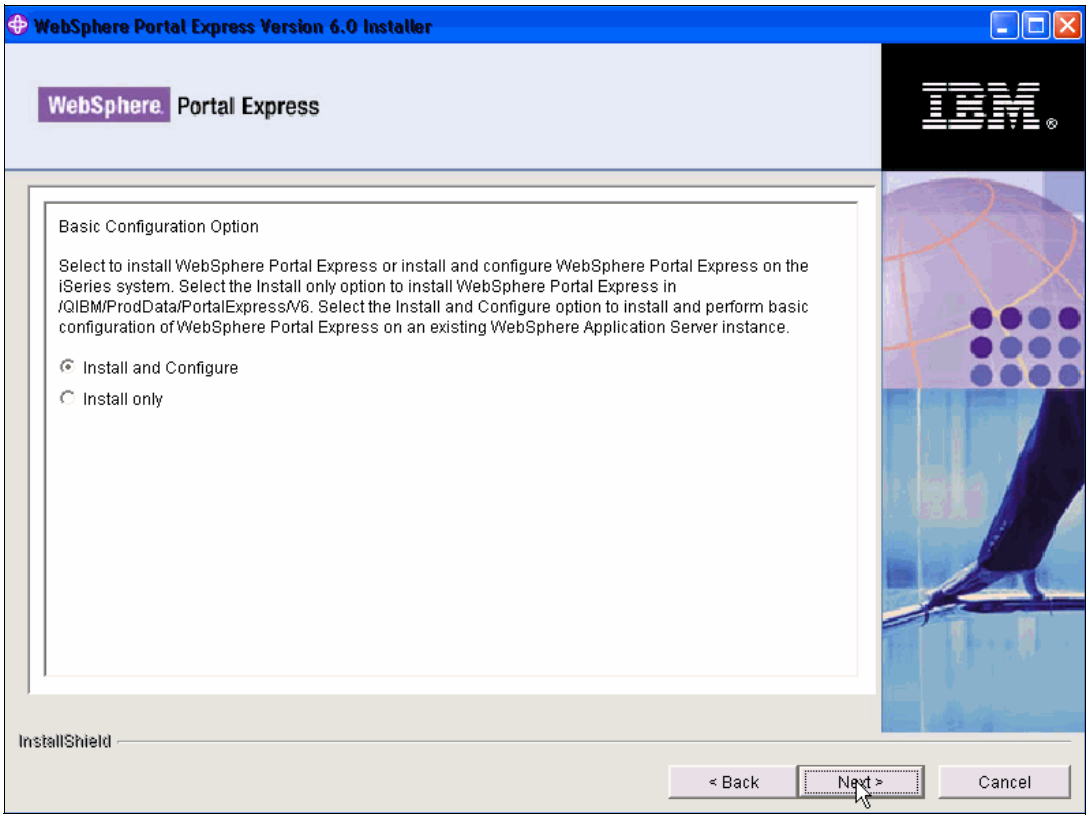

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
Basic Configuration Option
Select to install WebSphere Portal Express or install and configure WebSphere Portal Express on the iSeries system. Select the Install only option to install WebSphere Portal Express in /QIBM/ProdData/PortalExpress/V6. Select the Install and Configure option to install and perform basic configuration of WebSphere Portal Express on an existing WebSphere Application Server instance.
Install and Configure
Install only
InstallShield
< Back
Next >
Cancel

Figure 3-14 WebSphere Portal Express Install and Configure option

3. Select the WebSphere Application Server version (Figure 3-15) and click **Next**.

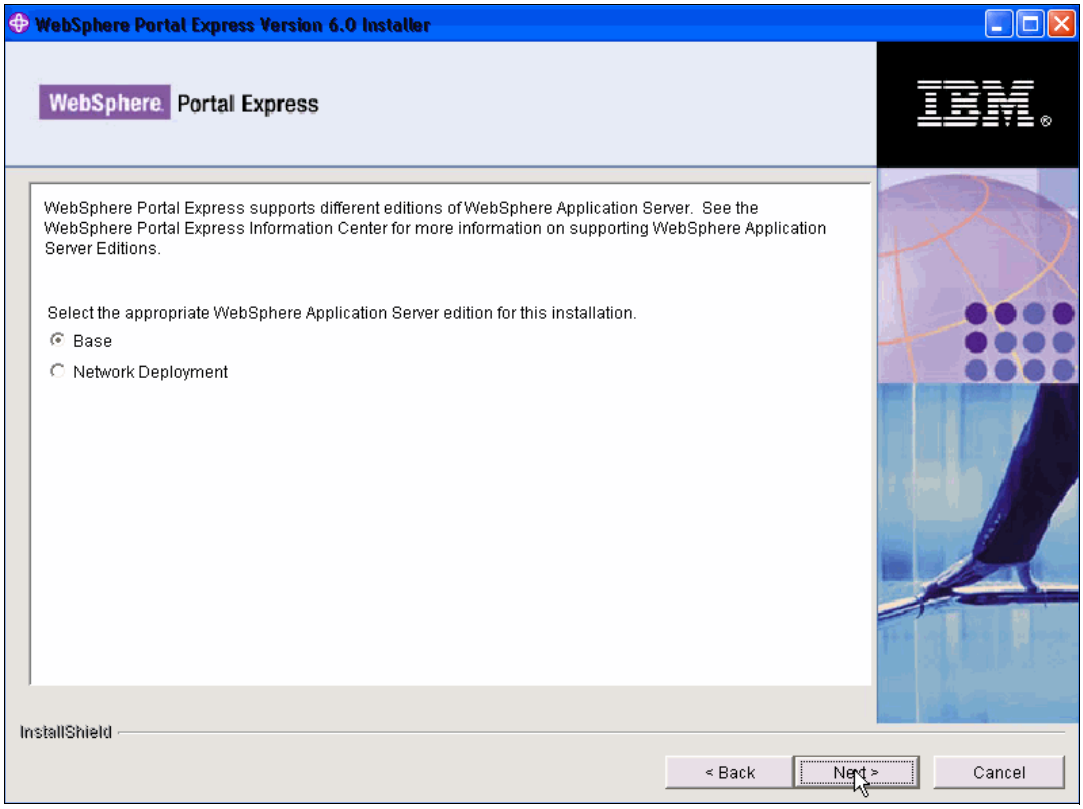

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
WebSphere Portal Express supports different editions of WebSphere Application Server. See the WebSphere Portal Express Information Center for more information on supporting WebSphere Application Server Editions.
Select the appropriate WebSphere Application Server edition for this installation.
Base
Network Deployment
InstallShield
< Back
Next >
Cancel

Figure 3-15 Selecting the WebSphere Application Server version

4. Enter the administrative user ID and password for the portal administrator and WebSphere Application Server administrator (Figure 3-16). The same user ID and password are used for both administrators.

Important: The password you enter in the window shown in Figure 3-16 is used for the user profile that owns the portal databases (wpdb2ins by default). The password *must* comply with your i5/OS password rules.

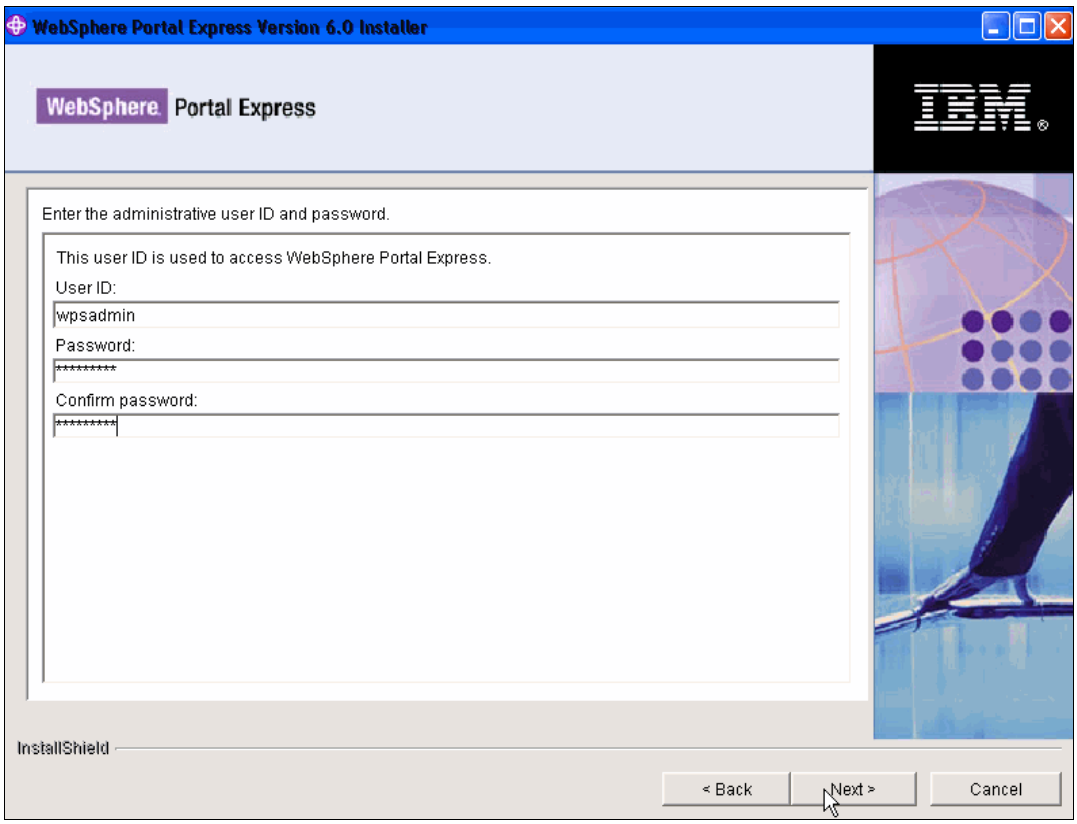


Figure 3-16 WebSphere Portal and WebSphere Application Server administrative user ID and password

5. WebSphere Portal Express is ready to install (Figure 3-17). Click **Next**.

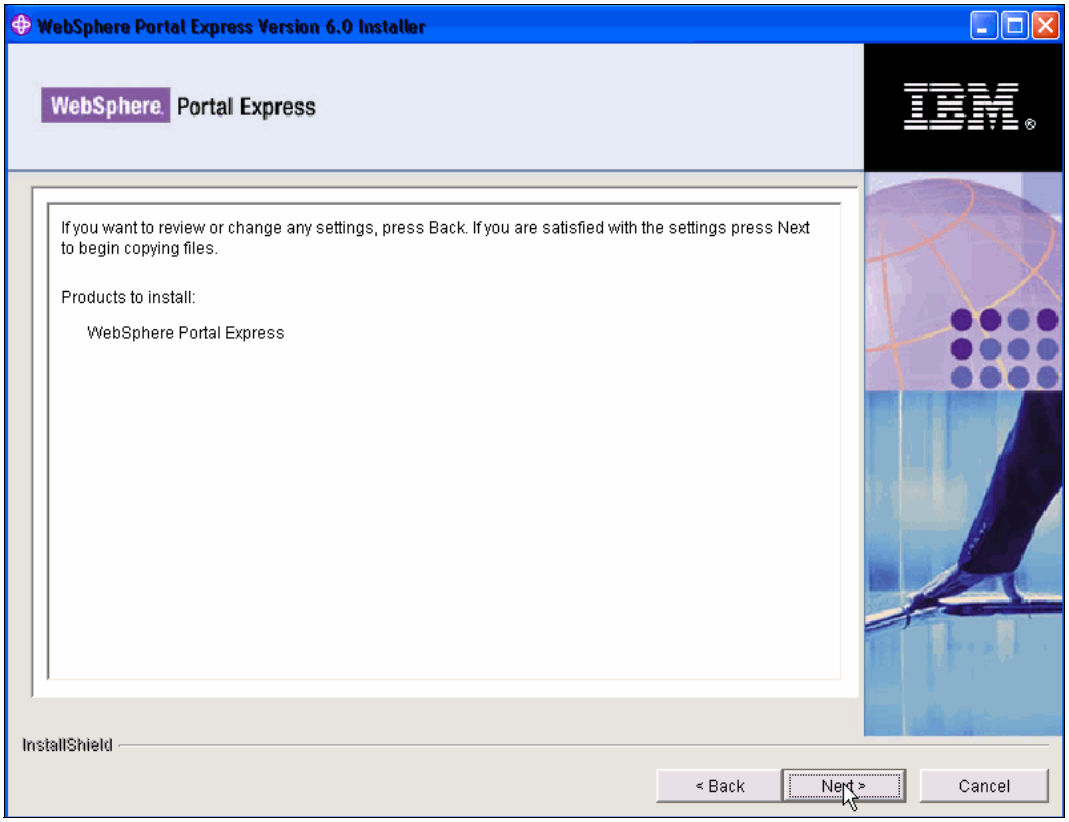

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
If you want to review or change any settings, press Back. If you are satisfied with the settings press Next to begin copying files.
Products to install:
WebSphere Portal Express
InstallShield
< Back
Next >
Cancel

Figure 3-17 WebSphere Portal Express ready to install

6. Notice the location of the installation logs as shown in Figure 3-18. Click **Next**.

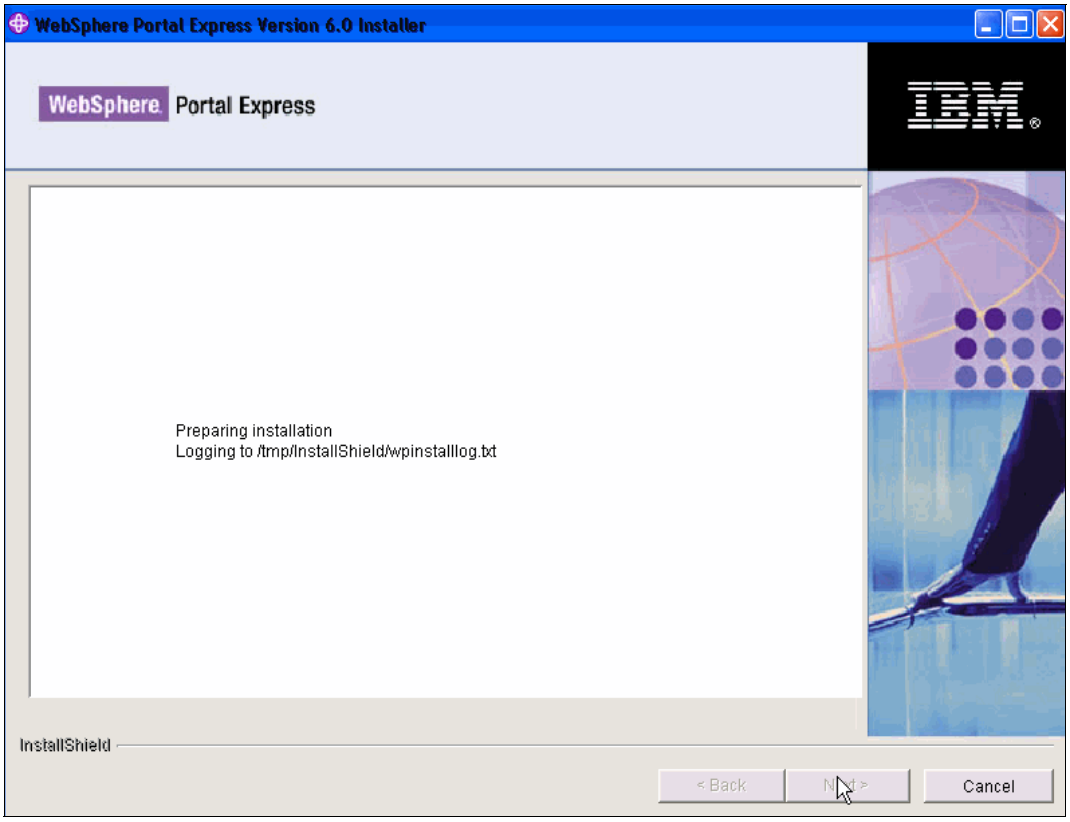


Figure 3-18 WebSphere Portal Express preparing the installation logs

7. The installation image files are copied to the i5/OS integrated file system directory of /QIBM/ProdData/PortalExpress/V6 as shown in Figure 3-19.

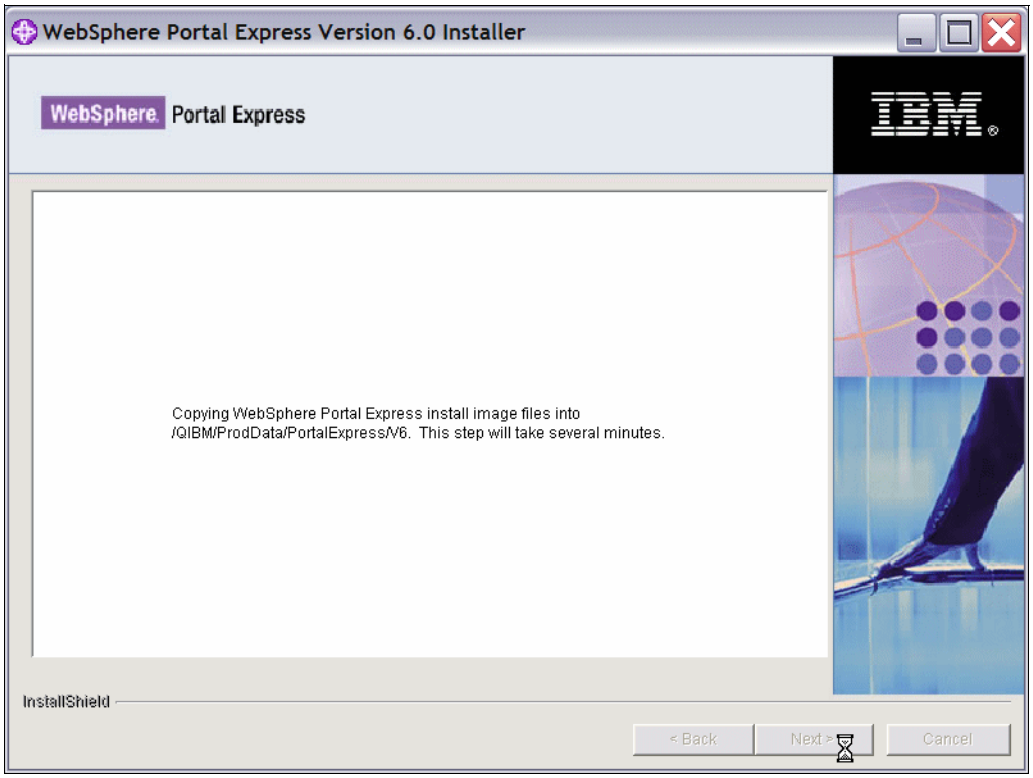


Figure 3-19 Copying the installation files to /QIBM/ProdData//PortalExpress/V6

8. The progress indicator shown in Figure 3-20 might not move during the extracting and configuring of the WebSphere Portal Express installation files; however, the installation is still in progress. Do not cancel it, just wait.

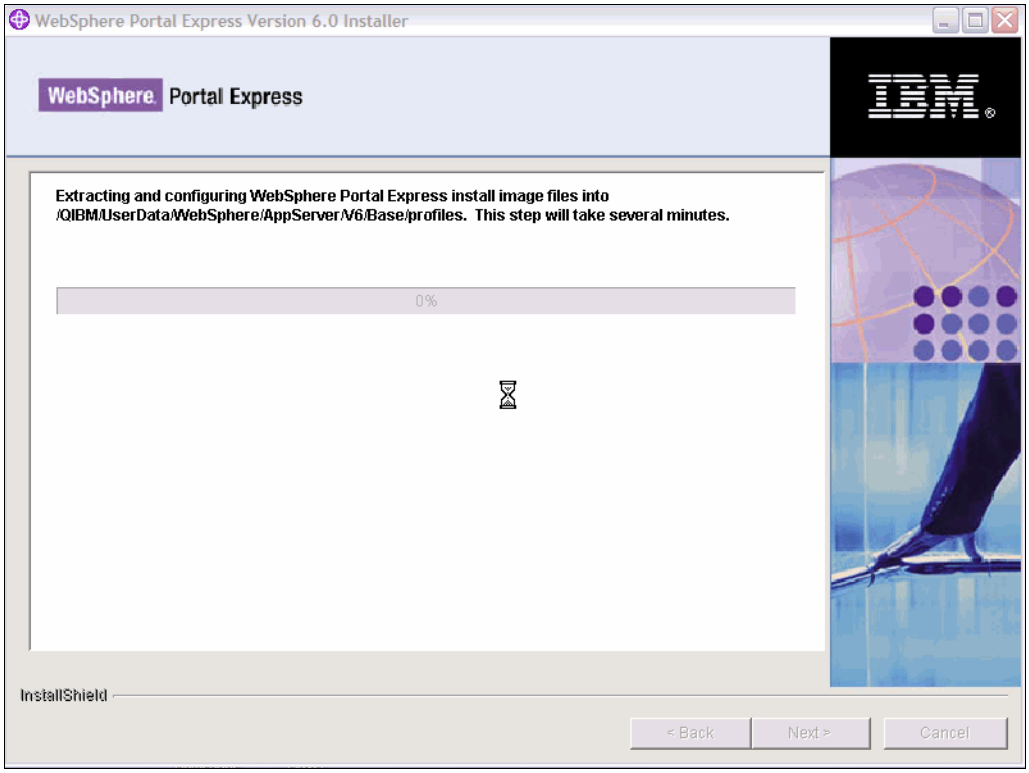

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
Extracting and configuring WebSphere Portal Express install image files into /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles. This step will take several minutes.
0%
InstallShield
< Back
Next >
Cancel

Figure 3-20 Extracting and configuring WebSphere Portal Express

9. After the installation has completed successfully as shown in Figure 3-21, copy the URL to access the portal from your Web browser.

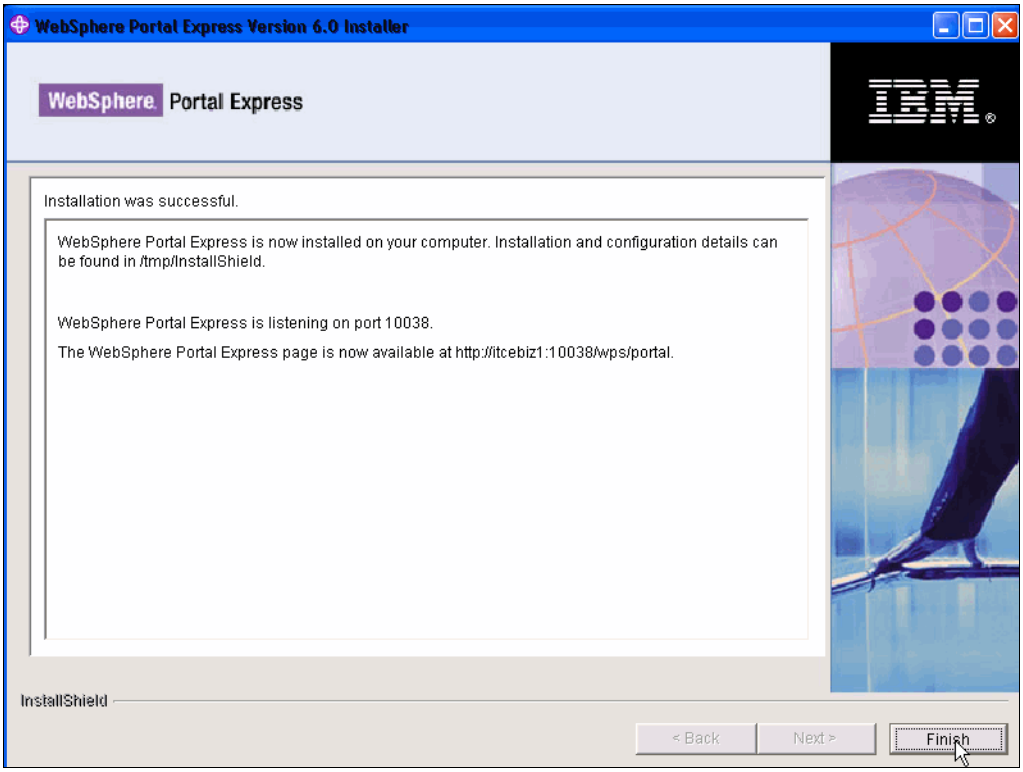

WebSphere Portal Express Version 6.0 Installer
WebSphere Portal Express
IBM
Installation was successful.
WebSphere Portal Express is now installed on your computer. Installation and configuration details can be found in /tmp/InstallShield.
WebSphere Portal Express is listening on port 10038.
The WebSphere Portal Express page is now available at http://itcebiz1:10038/wps/portal.
InstallShield
< Back
Next >
Finish

Figure 3-21 WebSphere Portal Express successful installation and configuration

10. At this point, see the WebSphere Portal V6 Information Center for details about configuring the HTTP and LDAP servers for your WebSphere Portal Express server.

    `http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp`

3.1.3 Common installation problems

This section includes information about common installation problems.

Prerequisites not verified properly

These issues are related to prerequisite products or PTFs missing or in `Failed` or `Not installed` status. Verify the prerequisite products and PTFs immediately before performing the WebSphere Portal Express installation and configuration. Refer to Chapter 2, “Preparing your i5/OS environment for WebSphere Portal Express” on page 15 for details.

Problems extracting electronic product images

These issues are related to problems downloading or extracting the electronic product images. For example, if you are installing from electronic images and you are prompted to install the next CD (see Figure 3-22 on page 68), there might be a problem with the files extracted in your download directory.

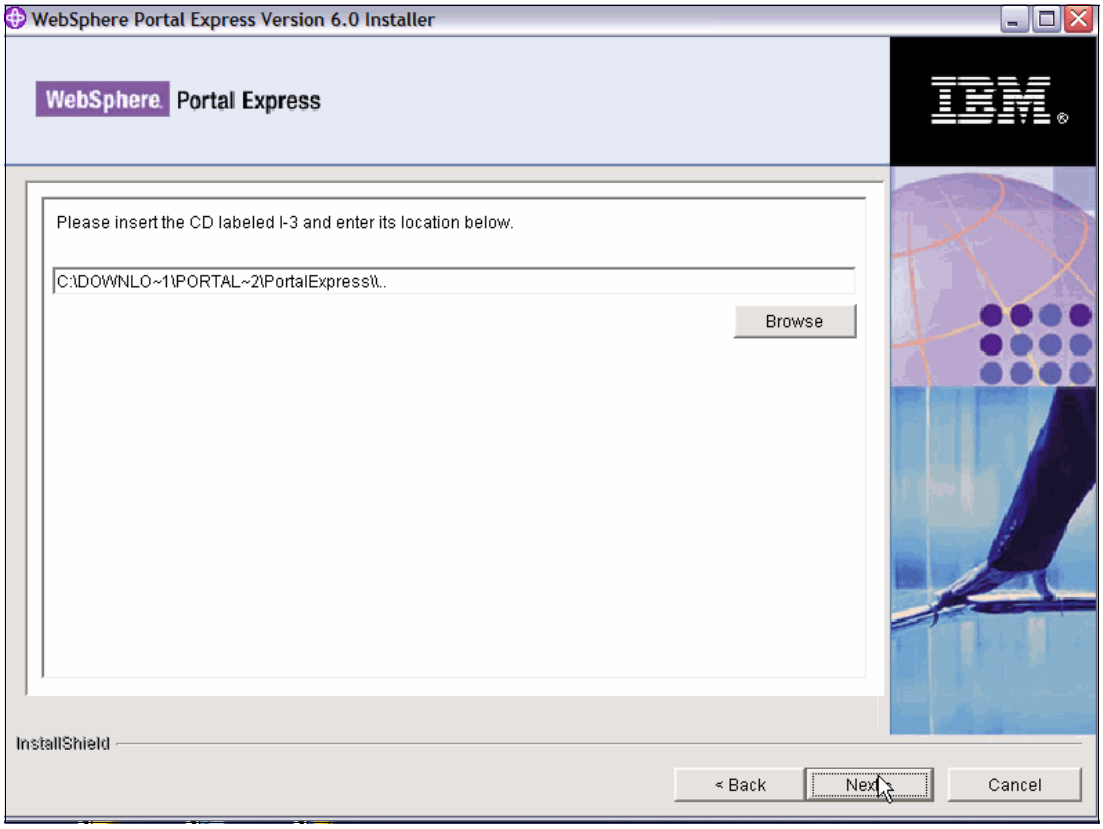


Figure 3-22 Electronic product images not extracted properly

Corrupted archive directories

One or more archive subdirectories in the \QIBM\ProdData\PortalExpress\V6\img directory is empty or has a file size of 0 bytes. Figure 3-23 shows that `archive1` is corrupted (empty) as an example of this problem.

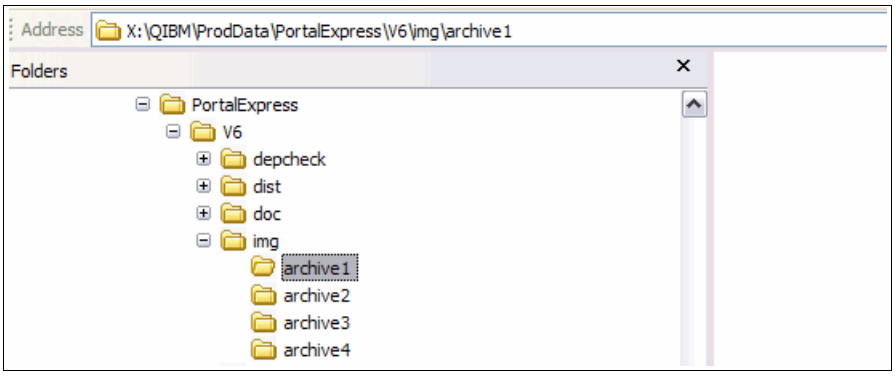


Figure 3-23 Corrupted archive1 directory in img subdirectory

If you run into this problem and are configuring portal with IBM Web Administration for i5/OS, you see the error shown in Figure 3-24 on page 69. If you run into this problem, uninstall and reinstall WebSphere Portal Express.

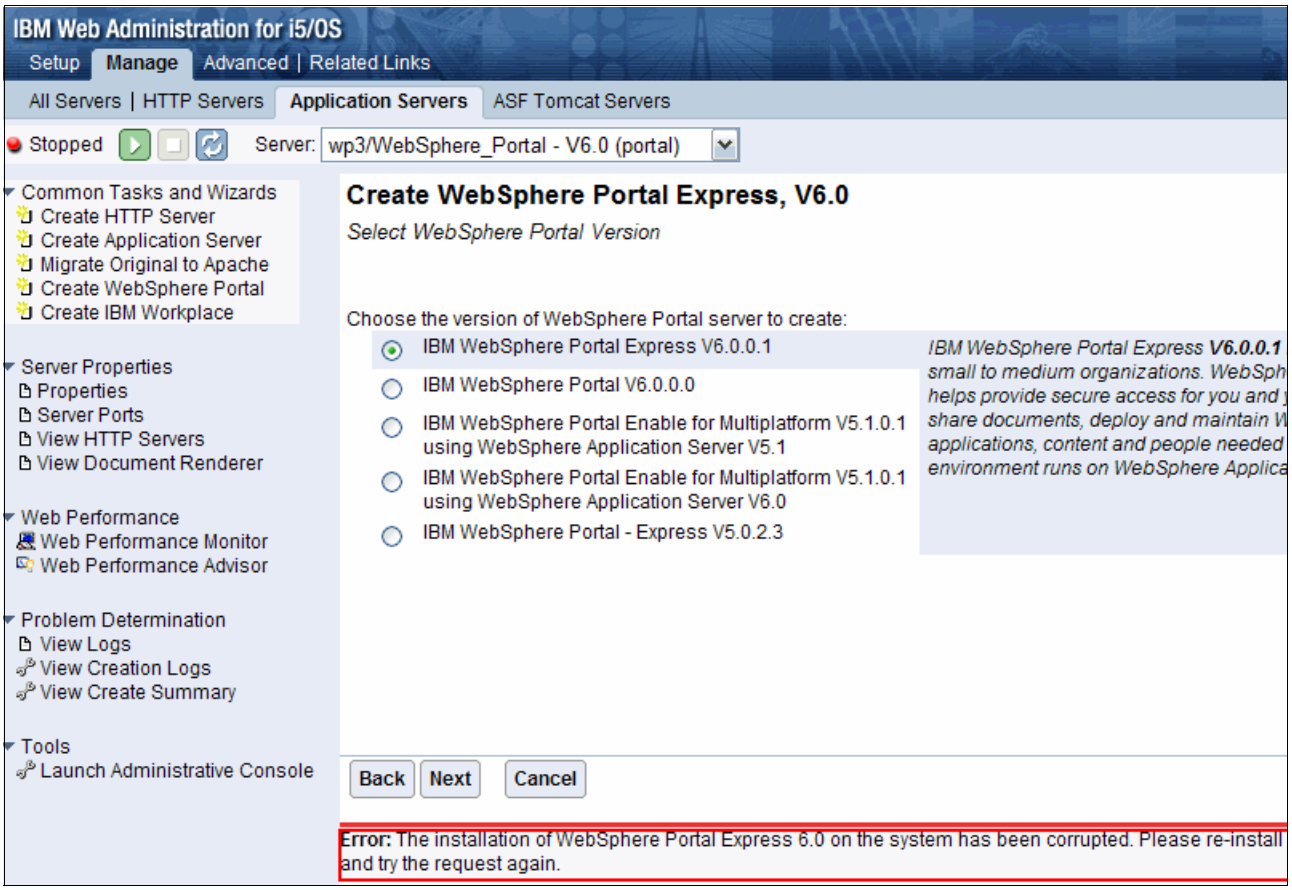


Figure 3-24 IBM Web Administration for i5/OS reporting corrupted installation

WebSphere Portal Express installation does not start after failed installation attempt

When the WebSphere Portal Express installation begins, the file /tmp/Installshield/portalinstall.lockfile is created in the i5/OS integrated file system and is removed after the installation has completed. If a previous attempt to install the product has not finished successfully, you might see an error message or notice that the installation does not proceed. If the file /tmp/Installshield/portalinstall.lockfile exists on your system, delete it before starting a new installation.

3.1.4 Verifying the WebSphere Portal Express installation

Perform the following steps to verify the successful installation of WebSphere Portal Express on i5/OS:

1. Check the product directory of \QIBM\ProdData\PortalExpress. Figure 3-25 on page 70 shows the directory structure after the installation.

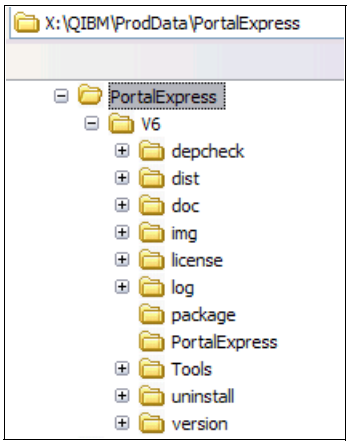


Figure 3-25 WebSphere Portal Express product directory

2. Verify that WebSphere Portal Express shows up in the i5/OS software inventory:
   a. Start the iSeries Navigator.
   b. Right-click the name of your System i machine.
   c. Select **Inventory** → **Collect**.
   d. Select **Software** and click **OK**.
   e. Expand **Management Central** and double-click **Endpoint Systems**.
   f. Double-click the name of your System i machine.
   g. Double-click **Configuration and Services**.
   h. Double-click **Software Inventory**.
   i. Double-click **Installed Products**.

   You see an entry of WebSphere Portal Express V6.0 as shown in Figure 3-26.

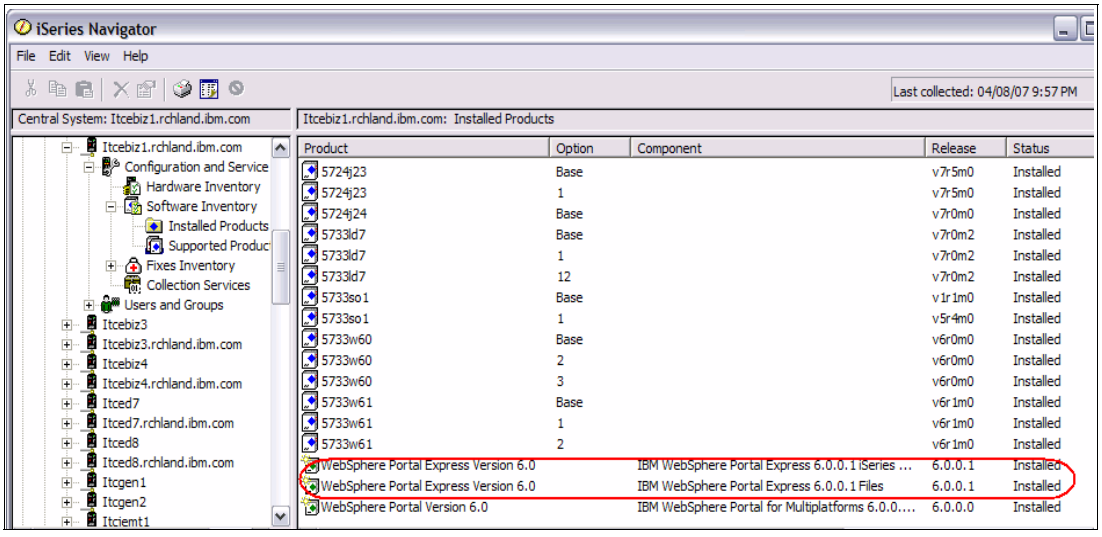

iSeries Navigator
File Edit View Help
Last collected: 04/08/07 9:57 PM
Central System: Itcebiz1.rchland.ibm.com
Itcebiz1.rchland.ibm.com: Installed Products
Product Option Component Release Status
WebSphere Portal Express Version 6.0 IBM WebSphere Portal Express 6.0.0.1 iSeries ... 6.0.0.1 Installed
WebSphere Portal Express Version 6.0 IBM WebSphere Portal Express 6.0.0.1 Files 6.0.0.1 Installed
WebSphere Portal Version 6.0 IBM WebSphere Portal for Multiplatforms 6.0.0.... 6.0.0.0 Installed

Figure 3-26 Software inventory: Installed products

3. Check the installation logs. Refer to 3.4.1, “Installation log files” on page 97 for a complete list of installation logs.

3.2 Configuring WebSphere Portal Express with IBM Web Administration for i5/OS

The Create WebSphere Portal wizard in IBM Web Administration for i5/OS supports WebSphere Portal Express V6 with the following PTFs:

- i5/OS V5R3:
  - 5722-DG1 SI27057 or PTF group SF99099 level 13
- i5/OS V5R4:
  - 5722-DG1 SI27058 or PTF group SF99114 level 8

The following limitations apply to WebSphere Portal Express profiles created with IBM Web Administration for i5/OS:

- Creation of the portal profile on WebSphere Application Server ND is not supported.
- Remote portal database is not supported.
- Microsoft Active Directory Application Mode (ADAM) 2003 is not supported.

3.2.1 Verifying the HTTP Administration server is active

The HTTP Administration server *must* be active to access the IBM Create WebSphere Portal Wizard for i5/OS from the IBM Web Administration for i5/OS. Perform the following steps to verify that the HTTP Administration server is active:

Start the HTTP Administration server on i5/OS using one of the following options:

1. Enter the following Start TCP/IP Server (STRTCPSVR) CL command:
   - `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`
   - From the iSeries Navigator, click **My Connections** → ***systemname*** → **Network** → **Servers** → **TCP/IP**. In the right pane, right-click **HTTP Administration** and click **Start** (Figure 3-27 on page 72).

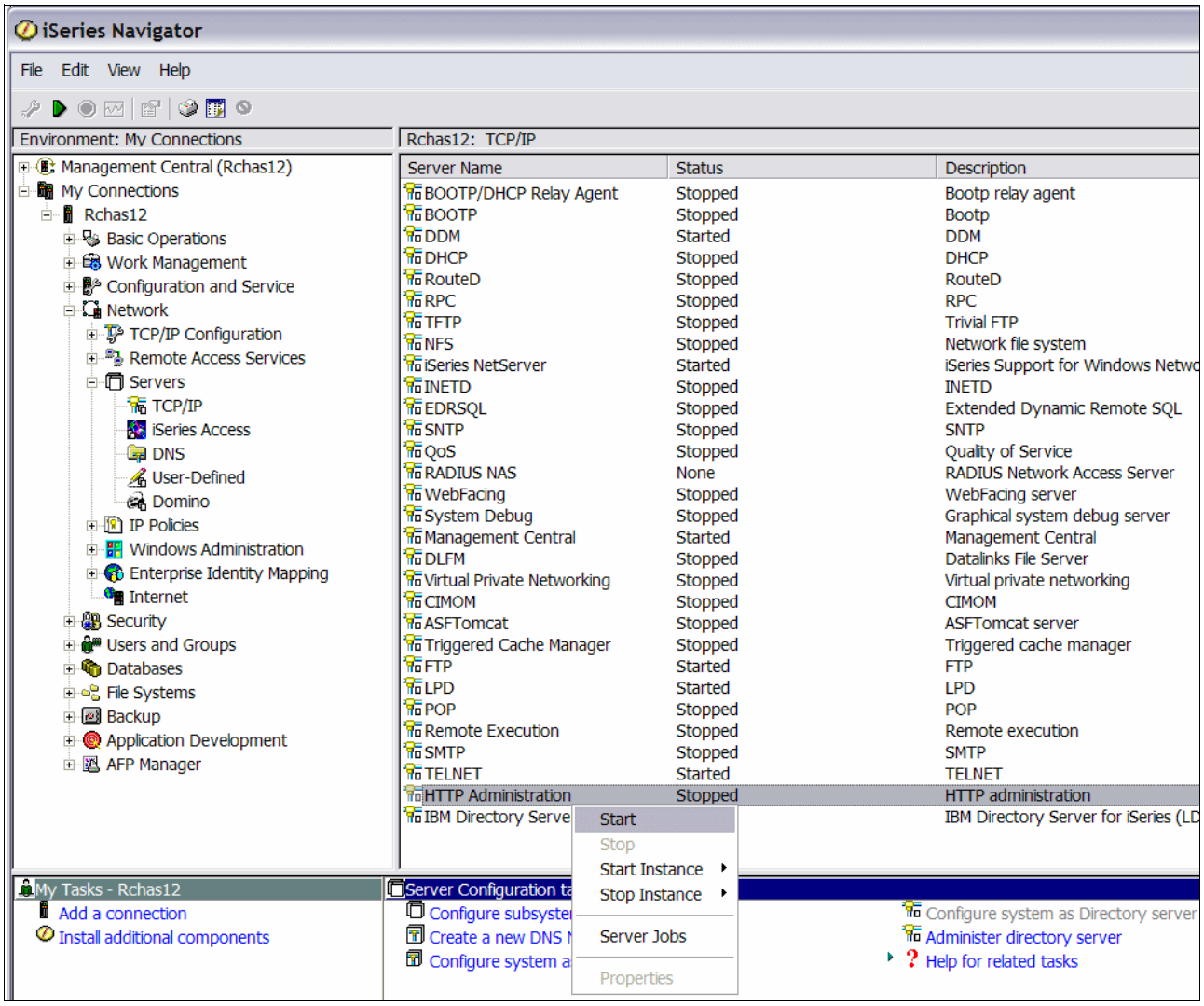


Figure 3-27 Starting the HTTP Administration server from iSeries Navigator

2. Access IBM Web Administration for i5/OS by pointing your Web browser to the following URL, where *system-hostname* is the fully qualified host name of your i5/OS instance:

   `http://system-hostname:2001`

   In this example, we use:

   `http://rchas10.rchland.ibm.com:2001`

3. When prompted, enter a valid i5/OS user profile and password with at least *ALLOBJ, *IOSYSCFG, and *JOBCTL special authorities. Click **OK**.

   Important: Do not use the QSECOFR user profile.

4. On the i5/OS Tasks Web page (Figure 3-28), click **IBM Web Administration for i5/OS**.

> **Note:** The options listed on the i5/OS Tasks Web page depend on the products that are installed in your i5/OS instance.

i5/OS Tasks - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://rchas10.rchland.ibm.com:2001/
Go
IBM
(C) IBM Corporation 2000
i5/OS Tasks
rchas10.rchland.ibm.com
IBM Web Administration for i5/OS
Configure HTTP servers, application servers and deploy applications
iSeries Navigator URL Advisor
Learn how to add i5/OS administration tasks into your web applications
Digital Certificate Manager
Create, distribute, and manage Digital Certificates
IBM Directory Server for i5/OS
Administer the IBM Directory Server
IBM IPP Server for i5/OS
Configure the IBM IPP Server
Cryptographic Coprocessor
Configure the cryptographic coprocessor
i5/OS Web-Based Help Server
Administer the Web-based help server
Related task information
Help
(Requires JavaScript)

Figure 3-28 i5/OS Tasks page

3.2.2 Configuring the WebSphere Portal profile

Perform the following steps to configure a WebSphere Portal profile using the Create WebSphere Portal for i5/OS wizard:

1. On the IBM Web Administration for i5/OS window, click **Create WebSphere Portal** (Figure 3-29 on page 74).

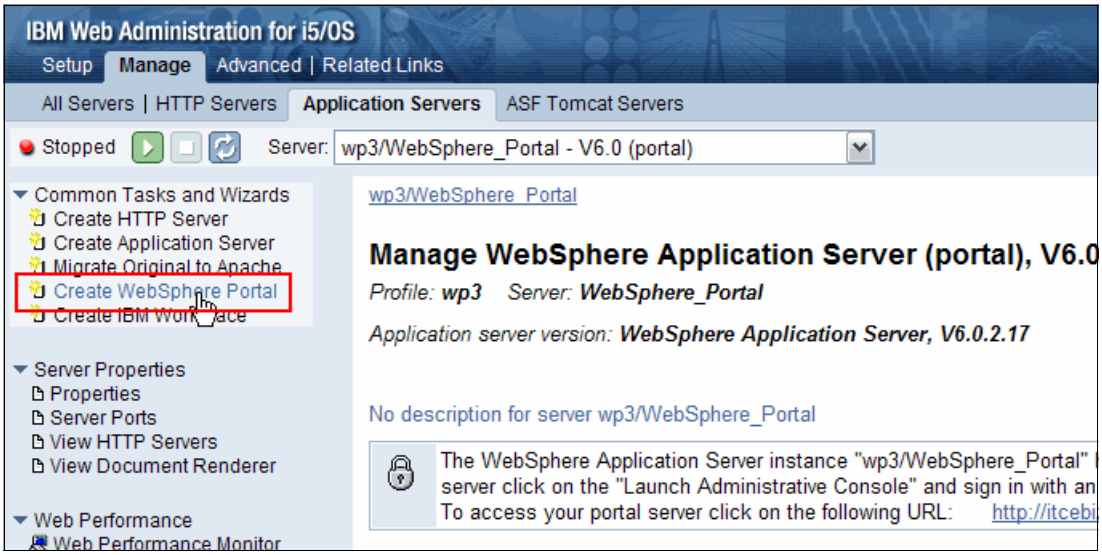


Figure 3-29 Creating a WebSphere Portal

2. On the Create WebSphere Portal window, click **Next** (Figure 3-30).

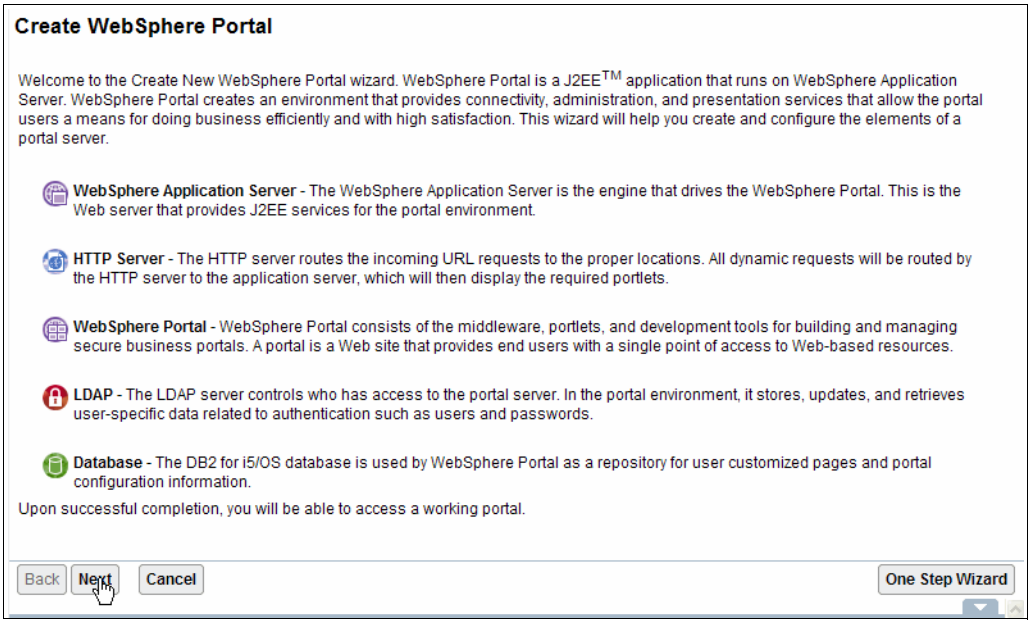

Create WebSphere Portal
Welcome to the Create New WebSphere Portal wizard. WebSphere Portal is a J2EE™ application that runs on WebSphere Application Server. WebSphere Portal creates an environment that provides connectivity, administration, and presentation services that allow the portal users a means for doing business efficiently and with high satisfaction. This wizard will help you create and configure the elements of a portal server.
WebSphere Application Server - The WebSphere Application Server is the engine that drives the WebSphere Portal. This is the Web server that provides J2EE services for the portal environment.
HTTP Server - The HTTP server routes the incoming URL requests to the proper locations. All dynamic requests will be routed by the HTTP server to the application server, which will then display the required portlets.
WebSphere Portal - WebSphere Portal consists of the middleware, portlets, and development tools for building and managing secure business portals. A portal is a Web site that provides end users with a single point of access to Web-based resources.
LDAP - The LDAP server controls who has access to the portal server. In the portal environment, it stores, updates, and retrieves user-specific data related to authentication such as users and passwords.
Database - The DB2 for i5/OS database is used by WebSphere Portal as a repository for user customized pages and portal configuration information.
Upon successful completion, you will be able to access a working portal.
Back
Next
Cancel
One Step Wizard

Figure 3-30 Continuing with creating a WebSphere Portal

3. Select **WebSphere Portal Express V6.0.0.1** and click **Next** (Figure 3-31).

Create WebSphere Portal
Select WebSphere Portal Version
Choose the version of WebSphere Portal server to create:
IBM WebSphere Portal Express V6.0.0.1
IBM WebSphere Portal V6.0.0.0
IBM WebSphere Portal Enable for Multiplatform V5.1.0.1 using WebSphere Application Server V5.1
IBM WebSphere Portal Enable for Multiplatform V5.1.0.1 using WebSphere Application Server V6.0
IBM WebSphere Portal - Express V5.0.2.3
IBM WebSphere Portal Express V6.0.0.1 is a portal solution sized for small to medium organizations. WebSphere Portal Express V6.0.0.1 helps provide secure access for you and your teams to collaborate and share documents, deploy and maintain Web sites, and access the applications, content and people needed for your job. This portal environment runs on WebSphere Application Server V6.0.
Back
Next
Cancel

Figure 3-31 Selecting the WebSphere Portal Express version

4. Enter the WebSphere Portal Express server name and click **Next** (Figure 3-32).

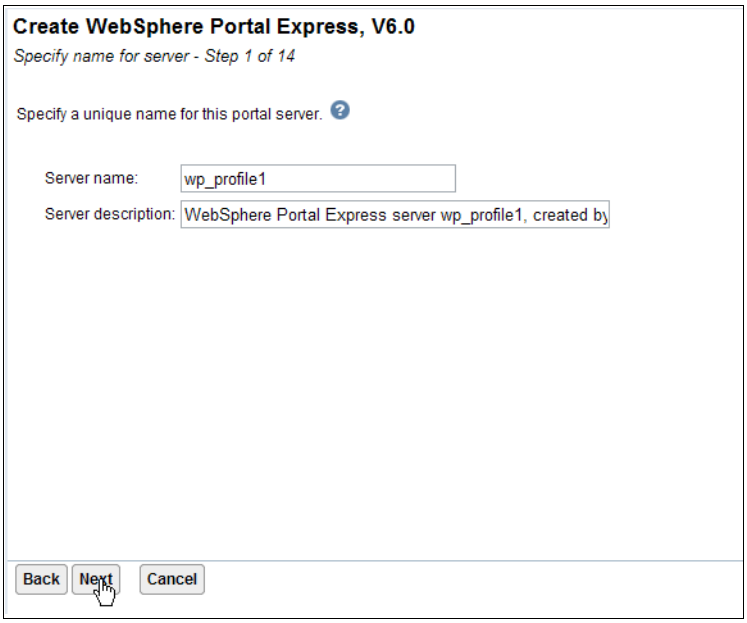


Figure 3-32 Entering the WebSphere Portal Express profile name

5. Specify the first port in the range to be assigned to the portal profile and click **Next**. The wizard verifies that the port range you specify is correct and that no port in the range is in use by active servers. If another WebSphere or HTTP server is configured using any of the ports in the specified range, an error message is displayed, and you cannot proceed until a range of free ports is chosen (Figure 3-33 on page 76).

Note: The wizard can check active ports and ports configured for HTTP and WebSphere servers even if the servers are not active. The wizard does not check configured but inactive ports for other applications, such as Domino.

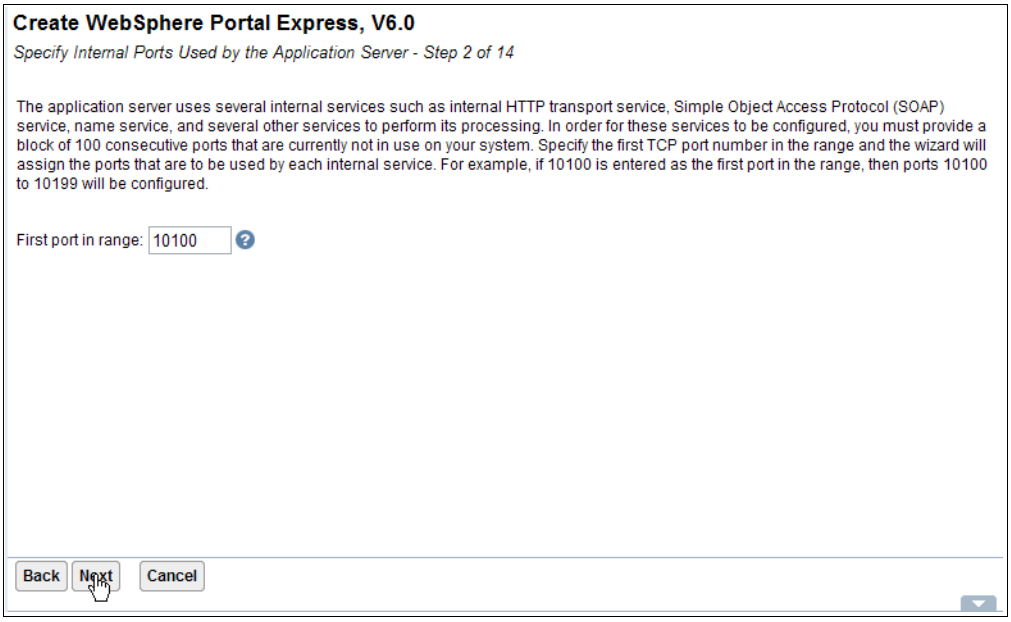

Create WebSphere Portal Express, V6.0
Specify Internal Ports Used by the Application Server - Step 2 of 14
The application server uses several internal services such as internal HTTP transport service, Simple Object Access Protocol (SOAP) service, name service, and several other services to perform its processing. In order for these services to be configured, you must provide a block of 100 consecutive ports that are currently not in use on your system. Specify the first TCP port number in the range and the wizard will assign the ports that are to be used by each internal service. For example, if 10100 is entered as the first port in the range, then ports 10100 to 10199 will be configured.
First port in range: 10100
Back
Next
Cancel

Figure 3-33 Specifying the first port of a free port range

6. Specify a user profile for the owner of the portal databases and select the naming convention for the portal databases (based on purpose or portal profile name). Click **Next** (Figure 3-34).

> **Important:** The user profile for the user that owns the databases *must* not exist. The password for this user profile is the same value as the portal administrator password, which is specified later in the wizard. This password must follow your System i password rules.

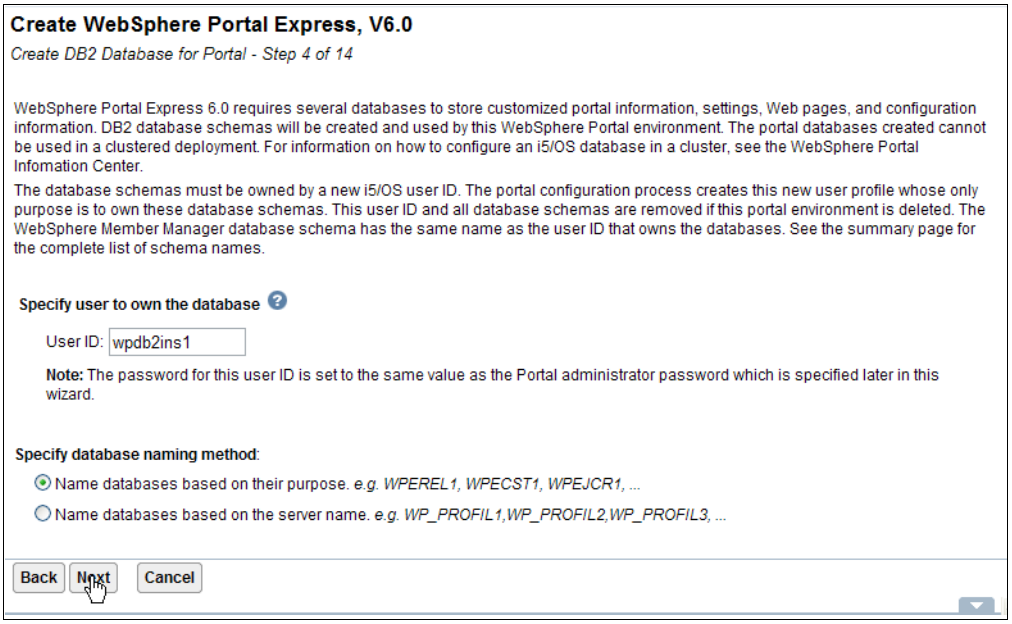

Create WebSphere Portal Express, V6.0
Create DB2 Database for Portal - Step 4 of 14
WebSphere Portal Express 6.0 requires several databases to store customized portal information, settings, Web pages, and configuration information. DB2 database schemas will be created and used by this WebSphere Portal environment. The portal databases created cannot be used in a clustered deployment. For information on how to configure an i5/OS database in a cluster, see the WebSphere Portal Infomation Center.
The database schemas must be owned by a new i5/OS user ID. The portal configuration process creates this new user profile whose only purpose is to own these database schemas. This user ID and all database schemas are removed if this portal environment is deleted. The WebSphere Member Manager database schema has the same name as the user ID that owns the databases. See the summary page for the complete list of schema names.
Specify user to own the database
User ID: wpdb2ins1
Note: The password for this user ID is set to the same value as the Portal administrator password which is specified later in this wizard.
Specify database naming method:
Name databases based on their purpose. e.g. WPEREL1, WPECST1, WPEJCR1, ...
Name databases based on the server name. e.g. WP_PROFIL1,WP_PROFIL2,WP_PROFIL3, ...
Back
Next
Cancel

Figure 3-34 Entering the database user ID and specifying the database naming method

7. Select **Do not use proxy** and click **Next** (Figure 3-35).

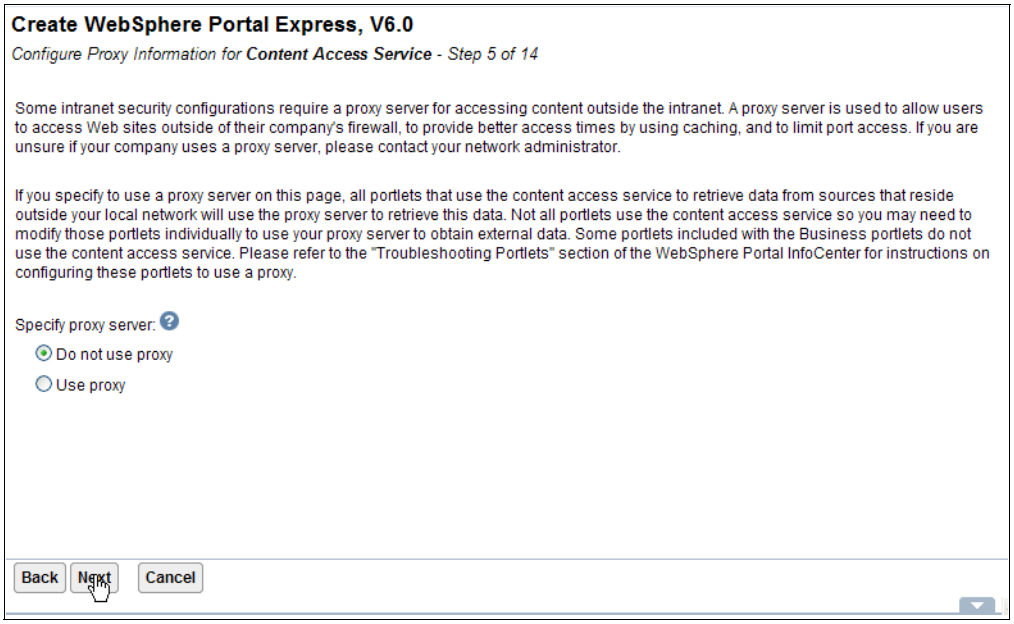

Create WebSphere Portal Express, V6.0
Configure Proxy Information for Content Access Service - Step 5 of 14
Some intranet security configurations require a proxy server for accessing content outside the intranet. A proxy server is used to allow users to access Web sites outside of their company's firewall, to provide better access times by using caching, and to limit port access. If you are unsure if your company uses a proxy server, please contact your network administrator.
If you specify to use a proxy server on this page, all portlets that use the content access service to retrieve data from sources that reside outside your local network will use the proxy server to retrieve this data. Not all portlets use the content access service so you may need to modify those portlets individually to use your proxy server to obtain external data. Some portlets included with the Business portlets do not use the content access service. Please refer to the "Troubleshooting Portlets" section of the WebSphere Portal InfoCenter for instructions on configuring these portlets to use a proxy.
Specify proxy server:
Do not use proxy
Use proxy
Back
Next
Cancel

Figure 3-35 Proxy information for content access service

8. Many of the portlets included in WebSphere Portal Express are deployed by default (Figure 3-36).

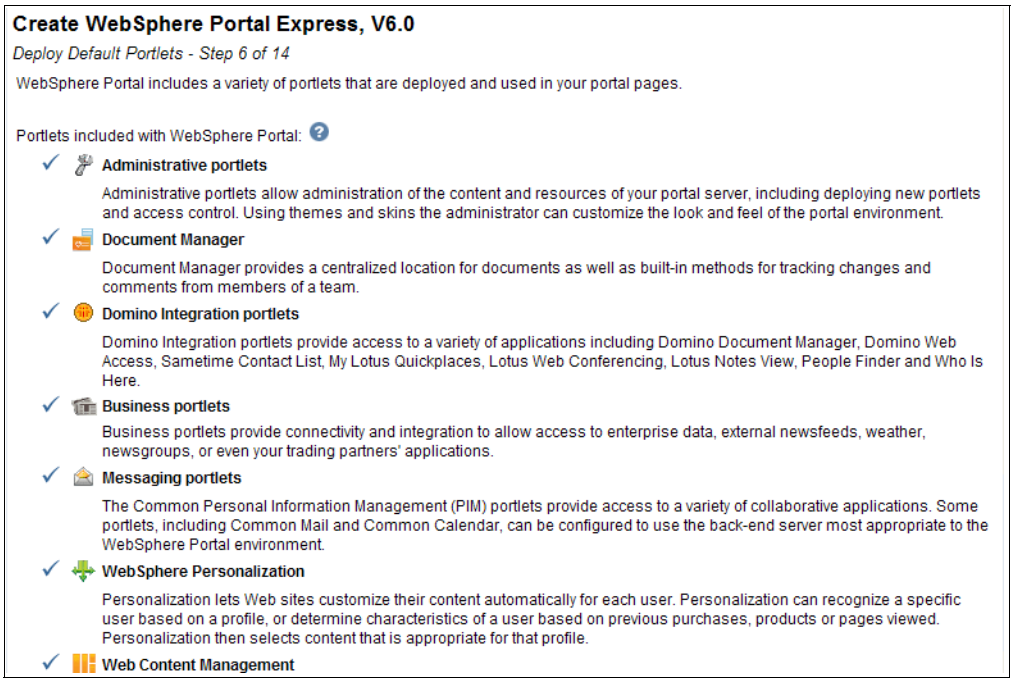

Create WebSphere Portal Express, V6.0
Deploy Default Portlets - Step 6 of 14
WebSphere Portal includes a variety of portlets that are deployed and used in your portal pages.
Portlets included with WebSphere Portal:
Administrative portlets
Administrative portlets allow administration of the content and resources of your portal server, including deploying new portlets and access control. Using themes and skins the administrator can customize the look and feel of the portal environment.
Document Manager
Document Manager provides a centralized location for documents as well as built-in methods for tracking changes and comments from members of a team.
Domino Integration portlets
Domino Integration portlets provide access to a variety of applications including Domino Document Manager, Domino Web Access, Sametime Contact List, My Lotus Quickplaces, Lotus Web Conferencing, Lotus Notes View, People Finder and Who Is Here.
Business portlets
Business portlets provide connectivity and integration to allow access to enterprise data, external newsfeeds, weather, newsgroups, or even your trading partners' applications.
Messaging portlets
The Common Personal Information Management (PIM) portlets provide access to a variety of collaborative applications. Some portlets, including Common Mail and Common Calendar, can be configured to use the back-end server most appropriate to the WebSphere Portal environment.
WebSphere Personalization
Personalization lets Web sites customize their content automatically for each user. Personalization can recognize a specific user based on a profile, or determine characteristics of a user based on previous purchases, products or pages viewed. Personalization then selects content that is appropriate for that profile.
Web Content Management

Figure 3-36 Deploy default portlets (1 of 2)

9. Select **Web Content Management Authoring** if you want to deploy the authoring environment in this portal profile. Select **iSeries Access for Web portlets** if you want to access information about your System i through the portal. Click **Next** (Figure 3-37).

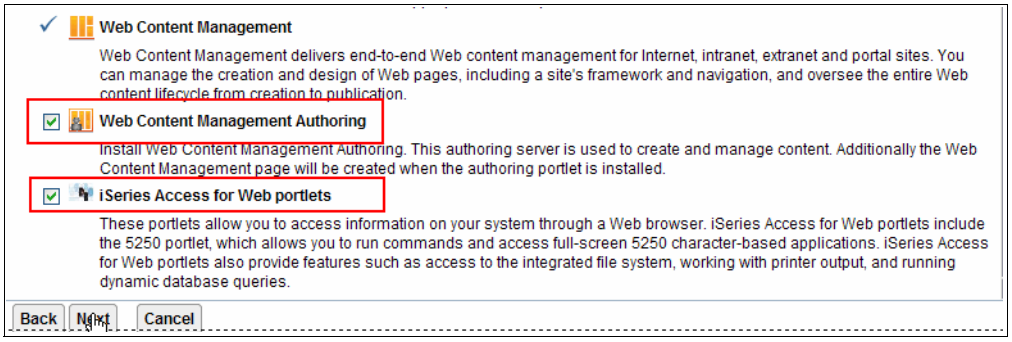

Web Content Management
Web Content Management delivers end-to-end Web content management for Internet, intranet, extranet and portal sites. You can manage the creation and design of Web pages, including a site's framework and navigation, and oversee the entire Web content lifecycle from creation to publication.
Web Content Management Authoring
Install Web Content Management Authoring. This authoring server is used to create and manage content. Additionally the Web Content Management page will be created when the authoring portlet is installed.
iSeries Access for Web portlets
These portlets allow you to access information on your system through a Web browser. iSeries Access for Web portlets include the 5250 portlet, which allows you to run commands and access full-screen 5250 character-based applications. iSeries Access for Web portlets also provide features such as access to the integrated file system, working with printer output, and running dynamic database queries.
Back
Next
Cancel

Figure 3-37 Selecting Web Content Management Authoring and iSeries Access for Web portlets

10. In this example, we are not showing the integration with Lotus Collaborative Components, therefore, do *not* select any of the collaborative components. Click **Next** (Figure 3-38).

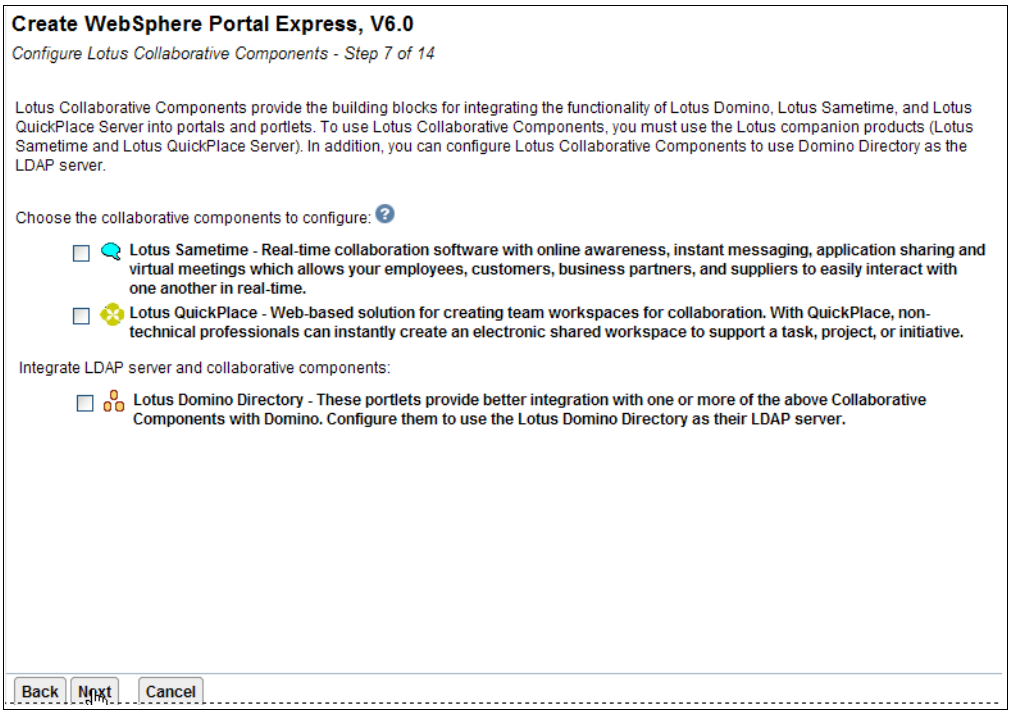

Create WebSphere Portal Express, V6.0
Configure Lotus Collaborative Components - Step 7 of 14
Lotus Collaborative Components provide the building blocks for integrating the functionality of Lotus Domino, Lotus Sametime, and Lotus QuickPlace Server into portals and portlets. To use Lotus Collaborative Components, you must use the Lotus companion products (Lotus Sametime and Lotus QuickPlace Server). In addition, you can configure Lotus Collaborative Components to use Domino Directory as the LDAP server.
Choose the collaborative components to configure:
Lotus Sametime - Real-time collaboration software with online awareness, instant messaging, application sharing and virtual meetings which allows your employees, customers, business partners, and suppliers to easily interact with one another in real-time.
Lotus QuickPlace - Web-based solution for creating team workspaces for collaboration. With QuickPlace, non-technical professionals can instantly create an electronic shared workspace to support a task, project, or initiative.
Integrate LDAP server and collaborative components:
Lotus Domino Directory - These portlets provide better integration with one or more of the above Collaborative Components with Domino. Configure them to use the Lotus Domino Directory as their LDAP server.
Back
Next
Cancel

Figure 3-38 Lotus Collaborative Components

11. Enter the LDAP server host name. By default, security is configured with realm support. Realm support allows you to configure virtual portals at a later time. You can also select to configure security using LDAP without realm support or to configure security using LDAP at a later time (Figure 3-39). In our example, we are using the IBM Directory Server that is included with i5/OS.

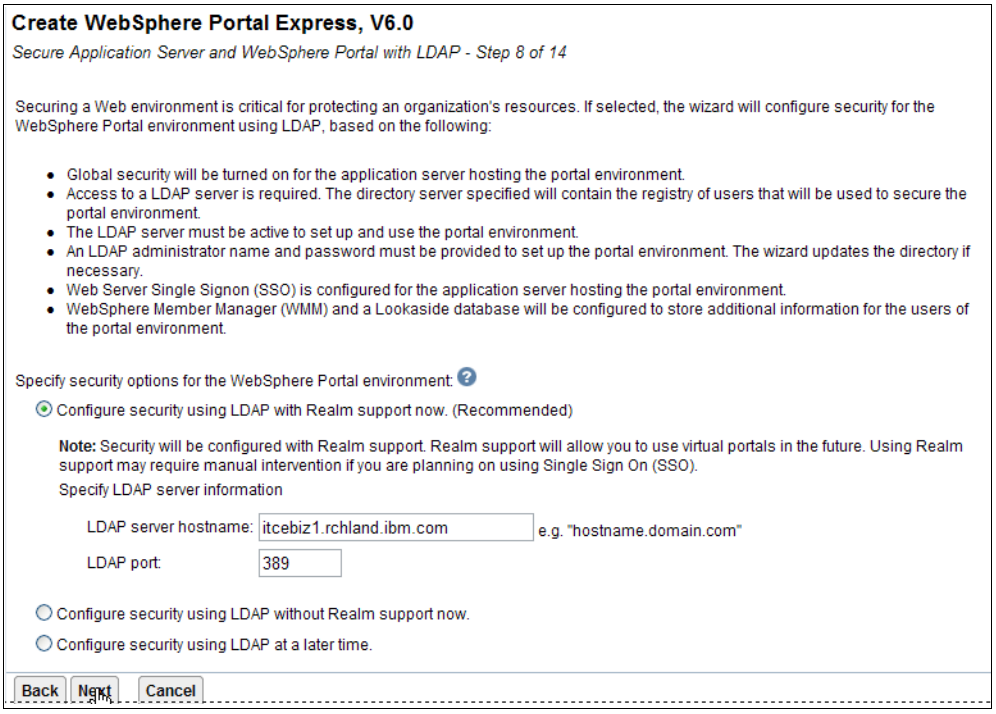

Create WebSphere Portal Express, V6.0
Secure Application Server and WebSphere Portal with LDAP - Step 8 of 14
Securing a Web environment is critical for protecting an organization's resources. If selected, the wizard will configure security for the WebSphere Portal environment using LDAP, based on the following:
Global security will be turned on for the application server hosting the portal environment.
Access to a LDAP server is required. The directory server specified will contain the registry of users that will be used to secure the portal environment.
The LDAP server must be active to set up and use the portal environment.
An LDAP administrator name and password must be provided to set up the portal environment. The wizard updates the directory if necessary.
Web Server Single Signon (SSO) is configured for the application server hosting the portal environment.
WebSphere Member Manager (WMM) and a Lookaside database will be configured to store additional information for the users of the portal environment.
Specify security options for the WebSphere Portal environment:
Configure security using LDAP with Realm support now. (Recommended)
Note: Security will be configured with Realm support. Realm support will allow you to use virtual portals in the future. Using Realm support may require manual intervention if you are planning on using Single Sign On (SSO).
Specify LDAP server information
LDAP server hostname: itcebiz1.rchland.ibm.com
e.g. "hostname.domain.com"
LDAP port: 389
Configure security using LDAP without Realm support now.
Configure security using LDAP at a later time.
Back
Next
Cancel

Figure 3-39 Securing WebSphere Application Server and WebSphere Portal with LDAP

12. Specify an LDAP user DN and password that has write access to the LDAP directory. We recommend that you use the LDAP administrator. If you cannot provide a user with write access to the directory, you *must* work with your LDAP administrator to prepare the LDAP directory for portal as described in 2.8, “Preparing the IBM Directory Server for i5/OS” on page 39 (Figure 3-40). Click **Next**.

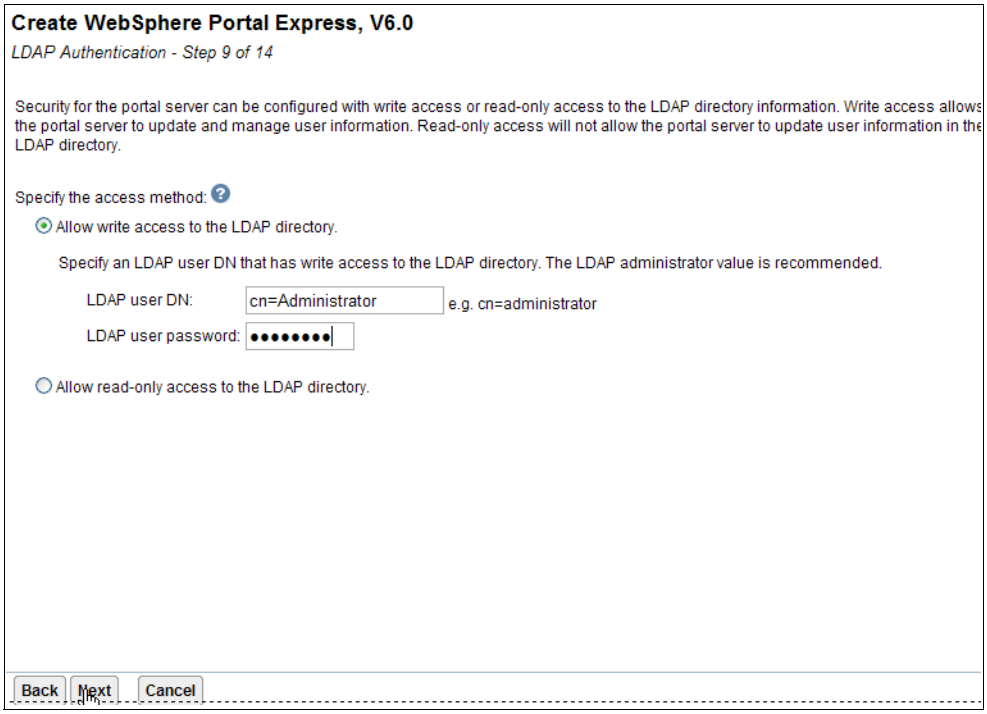

Create WebSphere Portal Express, V6.0
LDAP Authentication - Step 9 of 14
Security for the portal server can be configured with write access or read-only access to the LDAP directory information. Write access allows the portal server to update and manage user information. Read-only access will not allow the portal server to update user information in the LDAP directory.
Specify the access method:
Allow write access to the LDAP directory.
Specify an LDAP user DN that has write access to the LDAP directory. The LDAP administrator value is recommended.
LDAP user DN:
cn=Administrator
e.g. cn=administrator
LDAP user password:
Allow read-only access to the LDAP directory.
Back
Next
Cancel

Figure 3-40 LDAP authentication

13. The WebSphere Portal server utilizes LDAP to store user information for authentication purposes. The wizard creates the portal administrator user (for example, `wpsadmin`) and group (for example, `wpsadmins`) in the users and groups containers under the default LDAP suffix. If you want to use an LDAP suffix other than the default to store users and groups, you need to prepare the LDAP directory for portal as described in 2.8, “Preparing the IBM Directory Server for i5/OS” on page 39. Click **Next** if you are using the default LDAP suffix. For users, click **Browse** to select a parent DN other than the default suffix. See Figure 3-41.

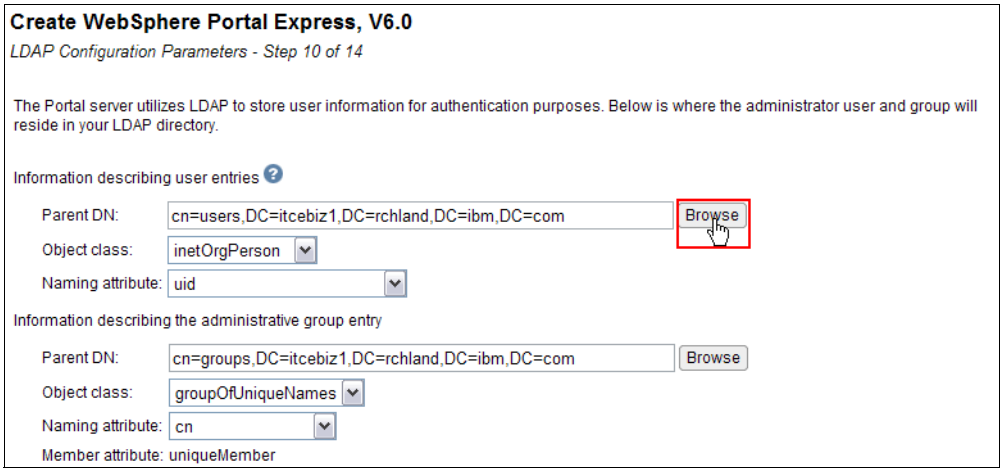


Figure 3-41 Selecting the parent DN for users

14. Figure 3-42 shows how to select a suffix for cn=users under a parent DN other than the default. Verify that cn=users, dc=…. appears at the bottom.

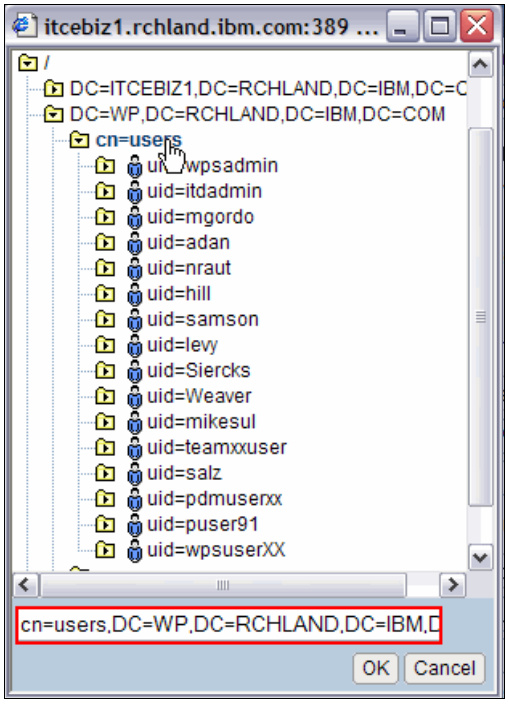


Figure 3-42 Browsing the LDAP directory to select the parent DN for cn=users

15. If you are using an LDAP suffix other than the default, click **Browse** in the Information describing the administrative group entry section (Figure 3-43). If you are using the LDAP suffix default, click **Next**.

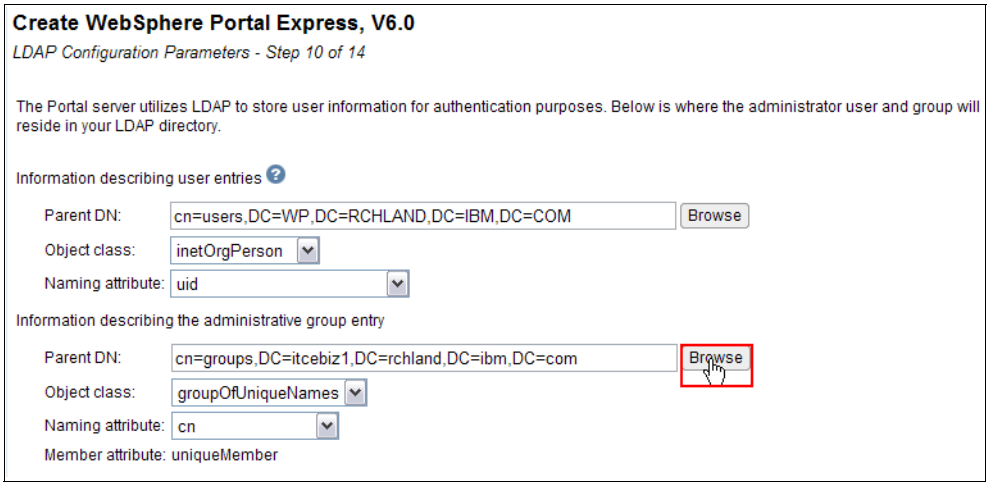


Figure 3-43 Selecting the parent DN for groups

16. Figure 3-44 shows how to select a suffix for cn=groups under a parent DN other than the default. Verify that cn=groups, dc=…. appears at the bottom.

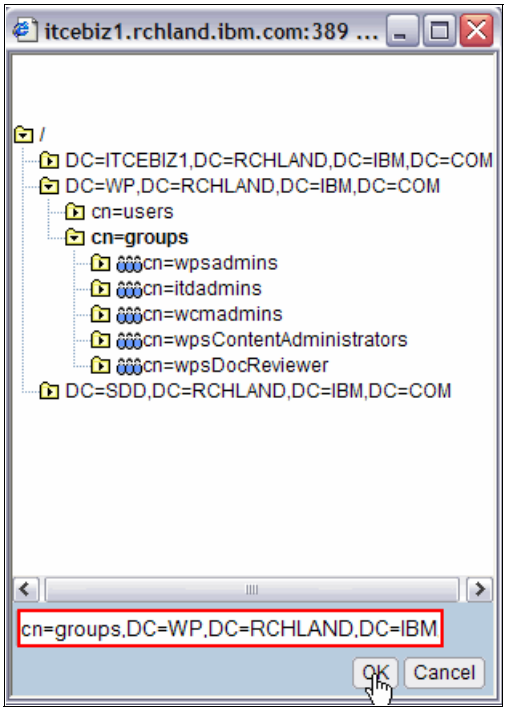


Figure 3-44 Browsing the LDAP directory to select the parent DN for cn=groups

17. Figure 3-45 shows the final LDAP user and groups selection. Click **Next**.

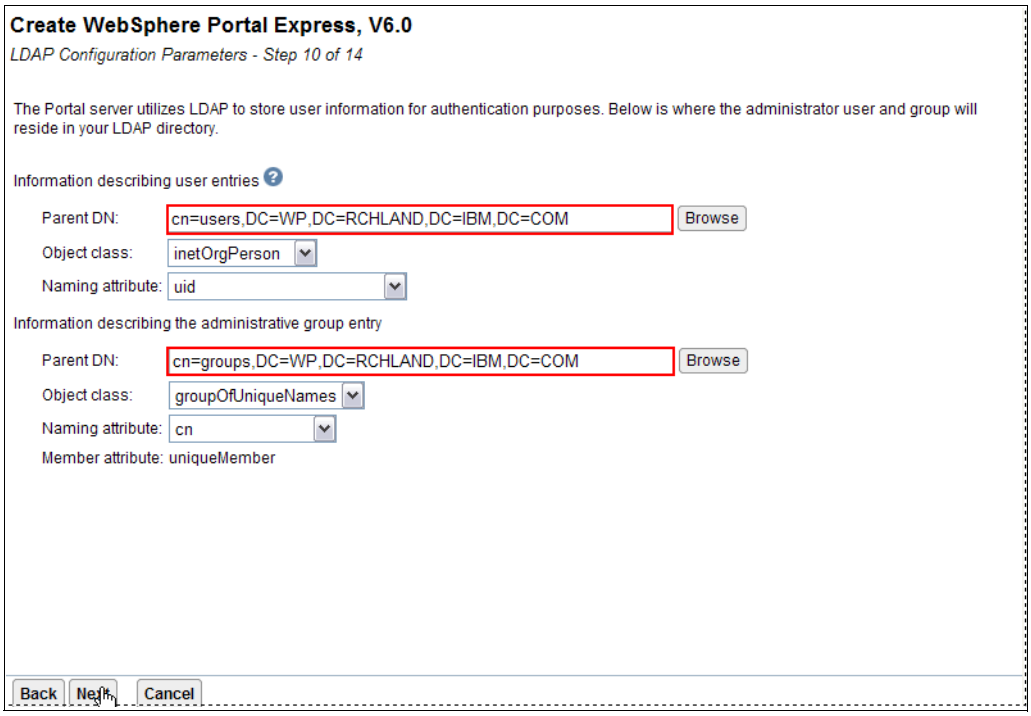

Create WebSphere Portal Express, V6.0
LDAP Configuration Parameters - Step 10 of 14
The Portal server utilizes LDAP to store user information for authentication purposes. Below is where the administrator user and group will reside in your LDAP directory.
Information describing user entries
Parent DN: cn=users,DC=WP,DC=RCHLAND,DC=IBM,DC=COM
Browse
Object class: inetOrgPerson
Naming attribute: uid
Information describing the administrative group entry
Parent DN: cn=groups,DC=WP,DC=RCHLAND,DC=IBM,DC=COM
Browse
Object class: groupOfUniqueNames
Naming attribute: cn
Member attribute: uniqueMember
Back
Next
Cancel

Figure 3-45 LDAP users and groups

18. Enter the password for the portal administrator, which is also the WebSphere Application Server administrator's user ID and password (Figure 3-46).

> **Important:** The password specified for this administrator is also used for the password of the database owner's user ID. The password *must* comply with your system password rules.

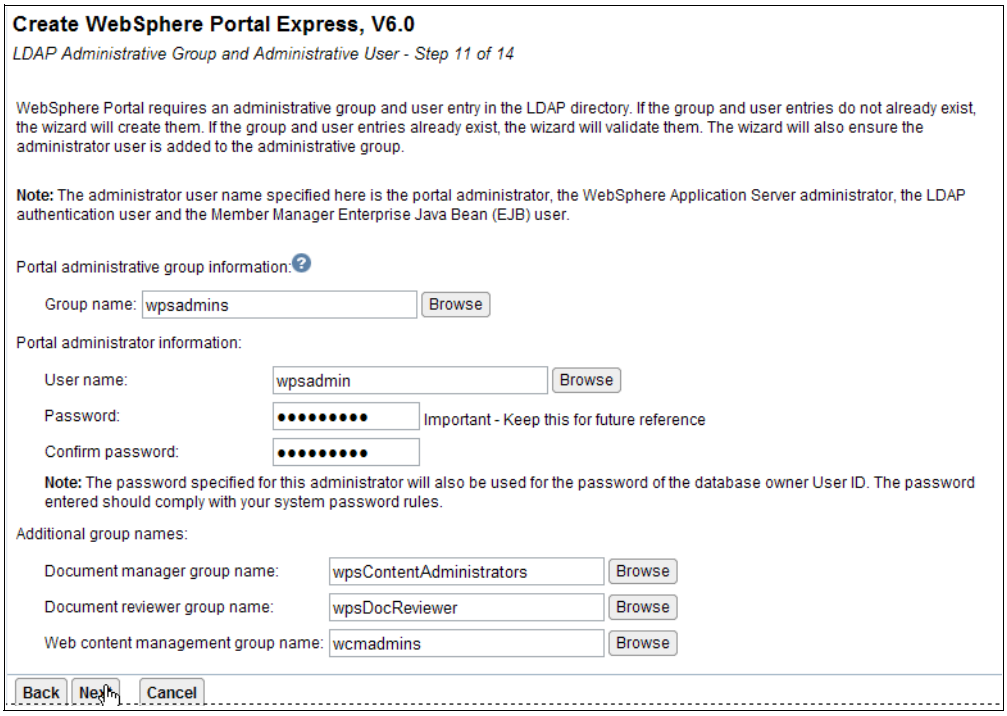

Create WebSphere Portal Express, V6.0
LDAP Administrative Group and Administrative User - Step 11 of 14
WebSphere Portal requires an administrative group and user entry in the LDAP directory. If the group and user entries do not already exist, the wizard will create them. If the group and user entries already exist, the wizard will validate them. The wizard will also ensure the administrator user is added to the administrative group.
Note: The administrator user name specified here is the portal administrator, the WebSphere Application Server administrator, the LDAP authentication user and the Member Manager Enterprise Java Bean (EJB) user.
Portal administrative group information:
Group name: wpsadmins
Browse
Portal administrator information:
User name: wpsadmin
Browse
Password:
Important - Keep this for future reference
Confirm password:
Note: The password specified for this administrator will also be used for the password of the database owner User ID. The password entered should comply with your system password rules.
Additional group names:
Document manager group name: wpsContentAdministrators
Browse
Document reviewer group name: wpsDocReviewer
Browse
Web content management group name: wcmadmins
Browse
Back
Next
Cancel

Figure 3-46 Portal administrative group information and portal administrator information

19. If you are not planning to configure single sign-on (SSO) with multiple Web servers, accept the defaults and click **Next** (Figure 3-47).

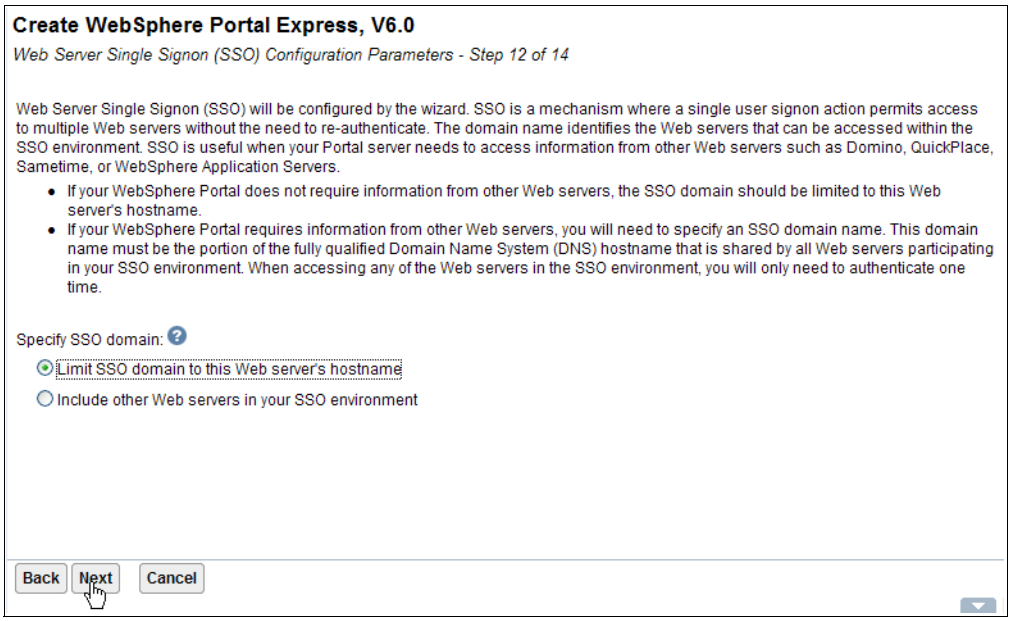

Create WebSphere Portal Express, V6.0
Web Server Single Signon (SSO) Configuration Parameters - Step 12 of 14
Web Server Single Signon (SSO) will be configured by the wizard. SSO is a mechanism where a single user signon action permits access to multiple Web servers without the need to re-authenticate. The domain name identifies the Web servers that can be accessed within the SSO environment. SSO is useful when your Portal server needs to access information from other Web servers such as Domino, QuickPlace, Sametime, or WebSphere Application Servers.
If your WebSphere Portal does not require information from other Web servers, the SSO domain should be limited to this Web server's hostname.
If your WebSphere Portal requires information from other Web servers, you will need to specify an SSO domain name. This domain name must be the portion of the fully qualified Domain Name System (DNS) hostname that is shared by all Web servers participating in your SSO environment. When accessing any of the Web servers in the SSO environment, you will only need to authenticate one time.
Specify SSO domain:
Limit SSO domain to this Web server's hostname
Include other Web servers in your SSO environment
Back
Next
Cancel

Figure 3-47 Web Server Single Sign-on (SSO) configuration

20. Select **Do not configure Identity Tokens** and click **Next** (Figure 3-48).

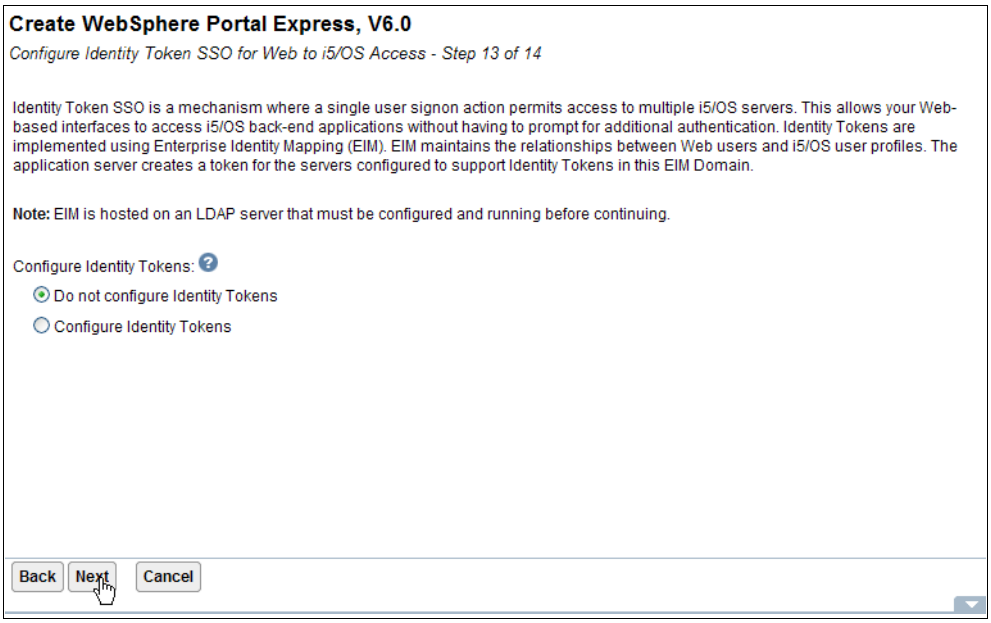

Create WebSphere Portal Express, V6.0
Configure Identity Token SSO for Web to i5/OS Access - Step 13 of 14
Identity Token SSO is a mechanism where a single user signon action permits access to multiple i5/OS servers. This allows your Web-based interfaces to access i5/OS back-end applications without having to prompt for additional authentication. Identity Tokens are implemented using Enterprise Identity Mapping (EIM). EIM maintains the relationships between Web users and i5/OS user profiles. The application server creates a token for the servers configured to support Identity Tokens in this EIM Domain.
Note: EIM is hosted on an LDAP server that must be configured and running before continuing.
Configure Identity Tokens:
Do not configure Identity Tokens
Configure Identity Tokens
Back
Next
Cancel

Figure 3-48 Configure Identity Token SSO for Web to i5/OS Access

21. Click **Printable Summary** to print a copy of your input to the configuration wizard. Review the configuration and click **Finish** (Figure 3-49).

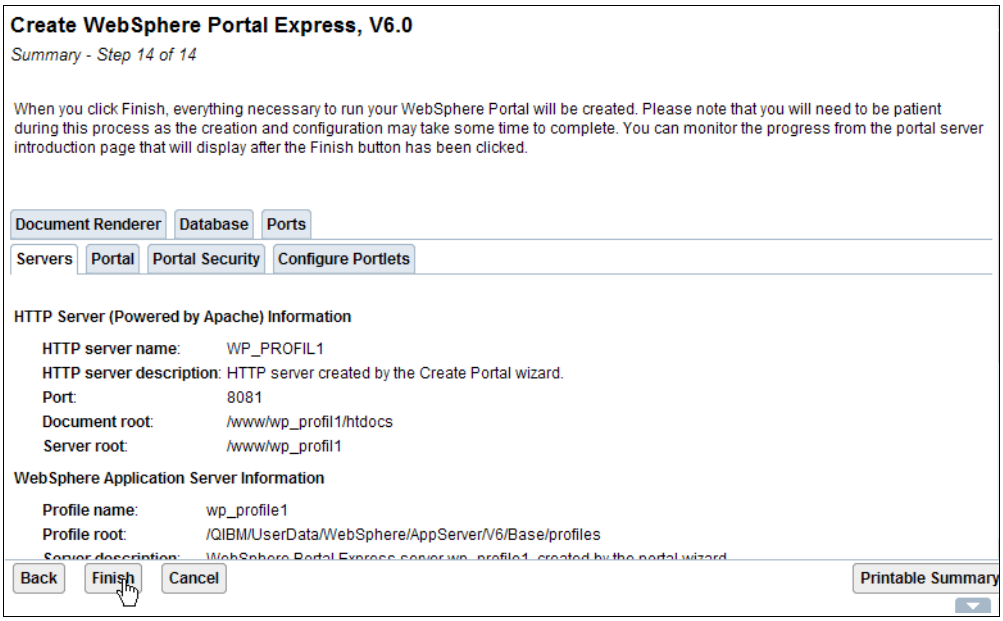

Create WebSphere Portal Express, V6.0
Summary - Step 14 of 14
When you click Finish, everything necessary to run your WebSphere Portal will be created. Please note that you will need to be patient during this process as the creation and configuration may take some time to complete. You can monitor the progress from the portal server introduction page that will display after the Finish button has been clicked.
Document Renderer
Database
Ports
Servers
Portal
Portal Security
Configure Portlets
HTTP Server (Powered by Apache) Information
HTTP server name: WP_PROFIL1
HTTP server description: HTTP server created by the Create Portal wizard.
Port: 8081
Document root: /www/wp_profil1/htdocs
Server root: /www/wp_profil1
WebSphere Application Server Information
Profile name: wp_profile1
Profile root: /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles
Back
Finish
Cancel
Printable Summary

Figure 3-49 Summary step

22. The process to complete the configuration will now run for a few hours (two to four hours, depending on the size of your system). You can close the Web browser and the configuration will continue. When the portal configuration ends, you can access the portal server by clicking the URL as shown in Figure 3-50.

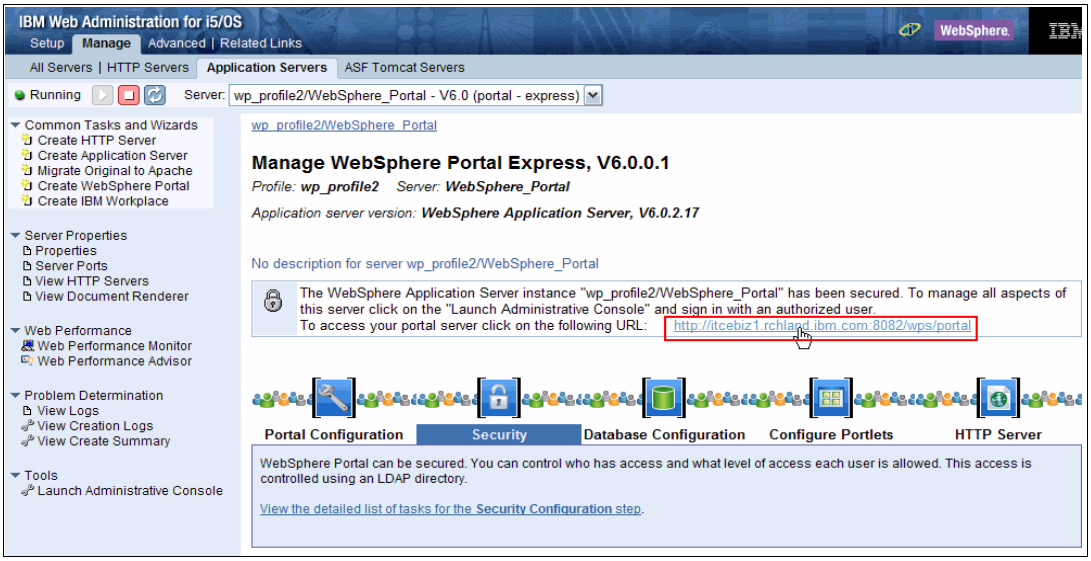

IBM Web Administration for i5/OS
Setup
Manage
Advanced | Related Links
WebSphere
All Servers | HTTP Servers
Application Servers
ASF Tomcat Servers
Running
Server: wp_profile2/WebSphere_Portal - V6.0 (portal - express)
Common Tasks and Wizards
Create HTTP Server
Create Application Server
Migrate Original to Apache
Create WebSphere Portal
Create IBM Workplace
Server Properties
Properties
Server Ports
View HTTP Servers
View Document Renderer
Web Performance
Web Performance Monitor
Web Performance Advisor
Problem Determination
View Logs
View Creation Logs
View Create Summary
Tools
Launch Administrative Console
wp_profile2/WebSphere_Portal
Manage WebSphere Portal Express, V6.0.0.1
Profile: wp_profile2 Server: WebSphere_Portal
Application server version: WebSphere Application Server, V6.0.2.17
No description for server wp_profile2/WebSphere_Portal
The WebSphere Application Server instance "wp_profile2/WebSphere_Portal" has been secured. To manage all aspects of this server click on the "Launch Administrative Console" and sign in with an authorized user.
To access your portal server click on the following URL: http://itcebiz1.rchland.ibm.com:8082/wps/portal
Portal Configuration
Security
Database Configuration
Configure Portlets
HTTP Server
WebSphere Portal can be secured. You can control who has access and what level of access each user is allowed. This access is controlled using an LDAP directory.
View the detailed list of tasks for the Security Configuration step.

Figure 3-50 Accessing the WebSphere Portal server

23. Log in to the portal and navigate through the pages and portlets (Figure 3-51).

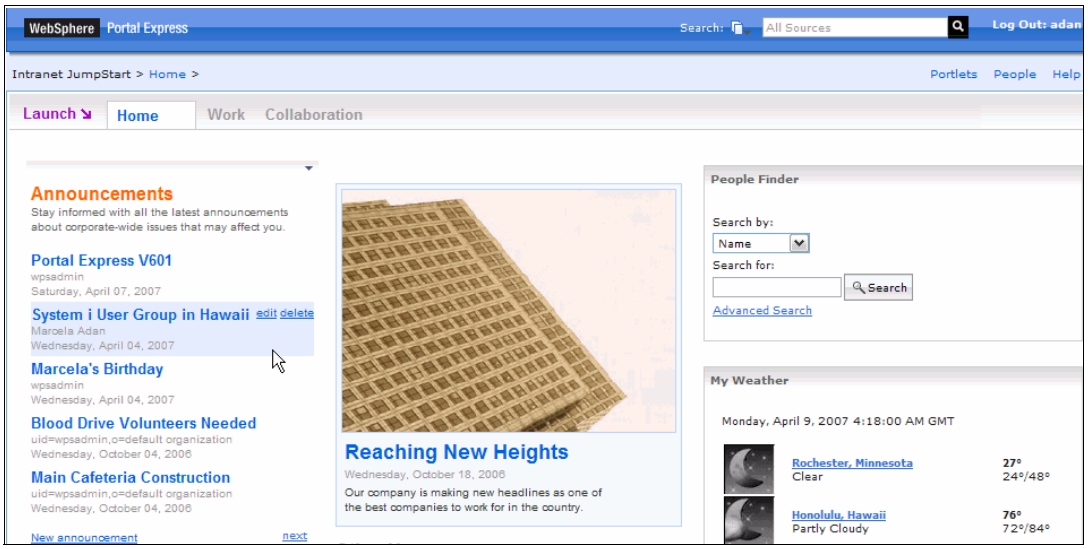


Figure 3-51 WebSphere Portal Express default home page

3.2.3 Accessing logs via IBM Web Administration for i5/OS

You can display the logs for a configuration step by placing the mouse over the step and clicking **View the detailed list of tasks** (Figure 3-52).

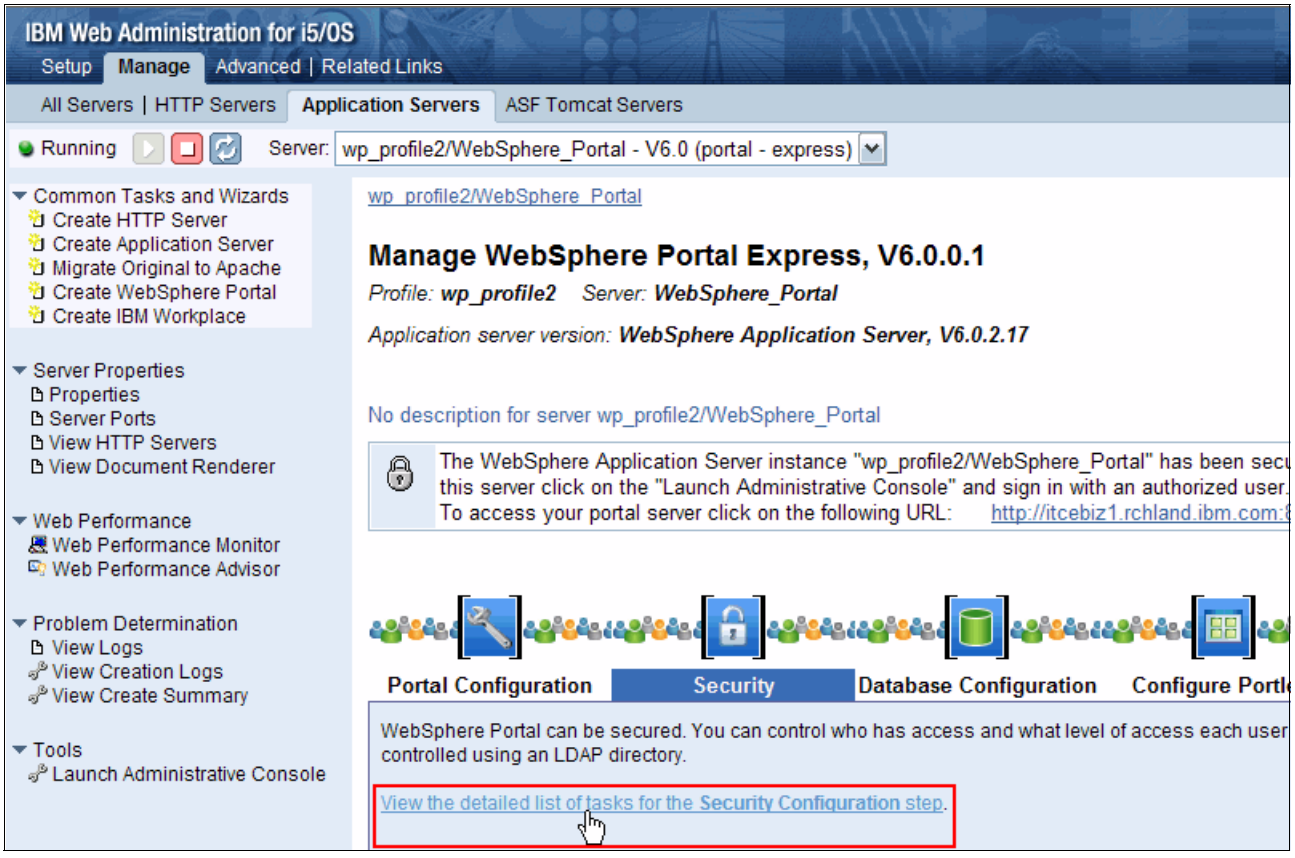

IBM Web Administration for i5/OS
Setup
Manage
Advanced | Related Links
All Servers | HTTP Servers
Application Servers
ASF Tomcat Servers
Running
Server: wp_profile2/WebSphere_Portal - V6.0 (portal - express)
Common Tasks and Wizards
Create HTTP Server
Create Application Server
Migrate Original to Apache
Create WebSphere Portal
Create IBM Workplace
Server Properties
Properties
Server Ports
View HTTP Servers
View Document Renderer
Web Performance
Web Performance Monitor
Web Performance Advisor
Problem Determination
View Logs
View Creation Logs
View Create Summary
Tools
Launch Administrative Console
wp_profile2/WebSphere_Portal
Manage WebSphere Portal Express, V6.0.0.1
Profile: wp_profile2 Server: WebSphere_Portal
Application server version: WebSphere Application Server, V6.0.2.17
No description for server wp_profile2/WebSphere_Portal
The WebSphere Application Server instance "wp_profile2/WebSphere_Portal" has been secu
this server click on the "Launch Administrative Console" and sign in with an authorized user.
To access your portal server click on the following URL:
Portal Configuration
Security
Database Configuration
Configure Portl
WebSphere Portal can be secured. You can control who has access and what level of access each user
controlled using an LDAP directory.
View the detailed list of tasks for the Security Configuration step.

Figure 3-52 Viewing the logs for a configuration task

Figure 3-53 shows the logs for the security configuration task.

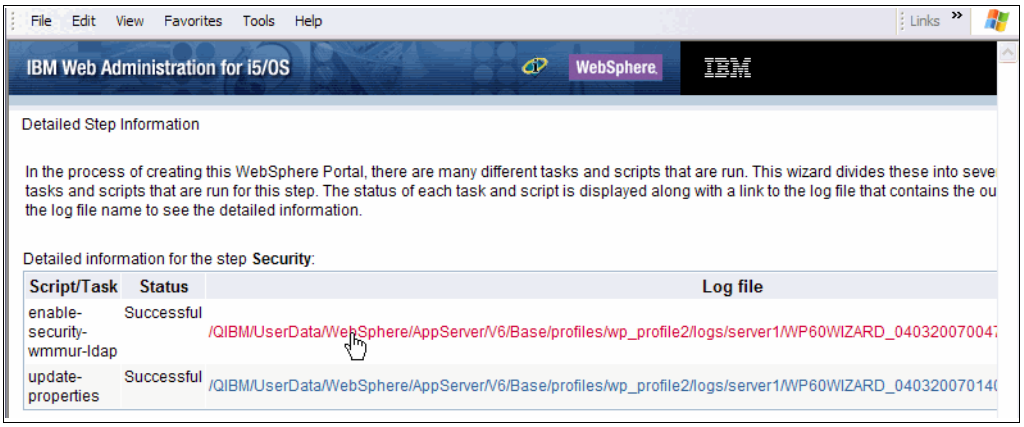

File Edit View Favorites Tools Help
Links
IBM Web Administration for i5/OS
WebSphere
IBM
Detailed Step Information
In the process of creating this WebSphere Portal, there are many different tasks and scripts that are run. This wizard divides these into seve
tasks and scripts that are run for this step. The status of each task and script is displayed along with a link to the log file that contains the ou
the log file name to see the detailed information.
Detailed information for the step Security:
Script/Task
Status
Log file
enable-security-wmmur-ldap
Successful
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wp_profile2/logs/server1/WP60WIZARD_04032007004
update-properties
Successful
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wp_profile2/logs/server1/WP60WIZARD_04032007014

Figure 3-53 Detailed step information

You can display all the WebSphere Application Server and WebSphere Portal Express logs associated with a portal profile at any time. Expand **Problem Determination**, click **View Logs,** and select the **WAS Logs** or **Portal Logs** tab (Figure 3-54).

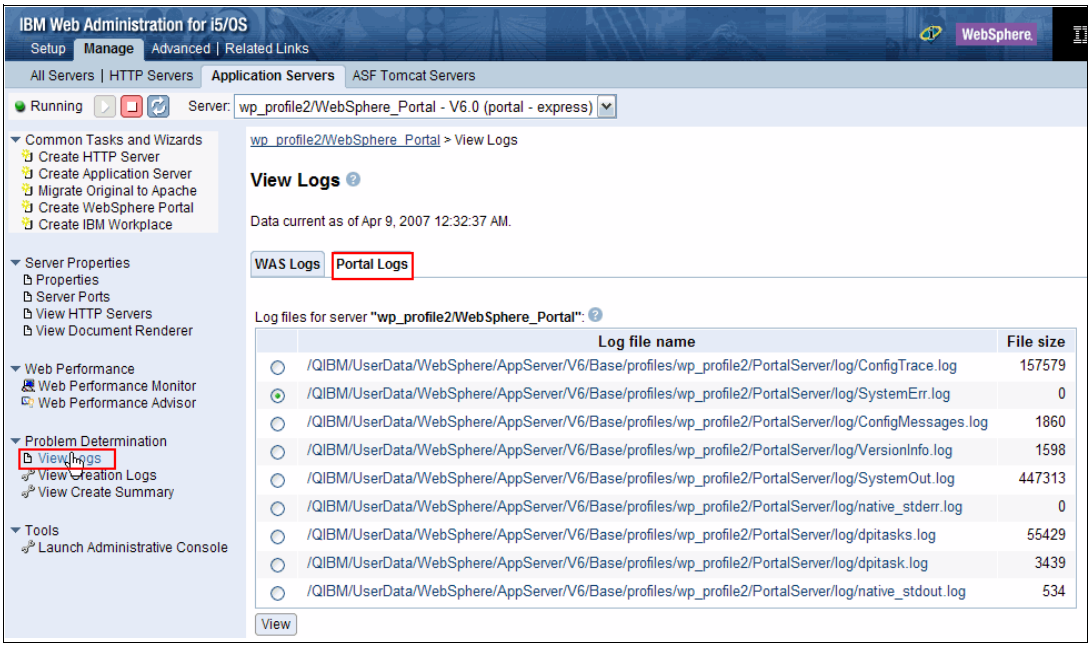


Figure 3-54 Viewing the WebSphere Application Server and WebSphere Portal logs

Click **View Creation Logs** to view detailed task information and error logs that were created during the portal configuration process (Figure 3-55).

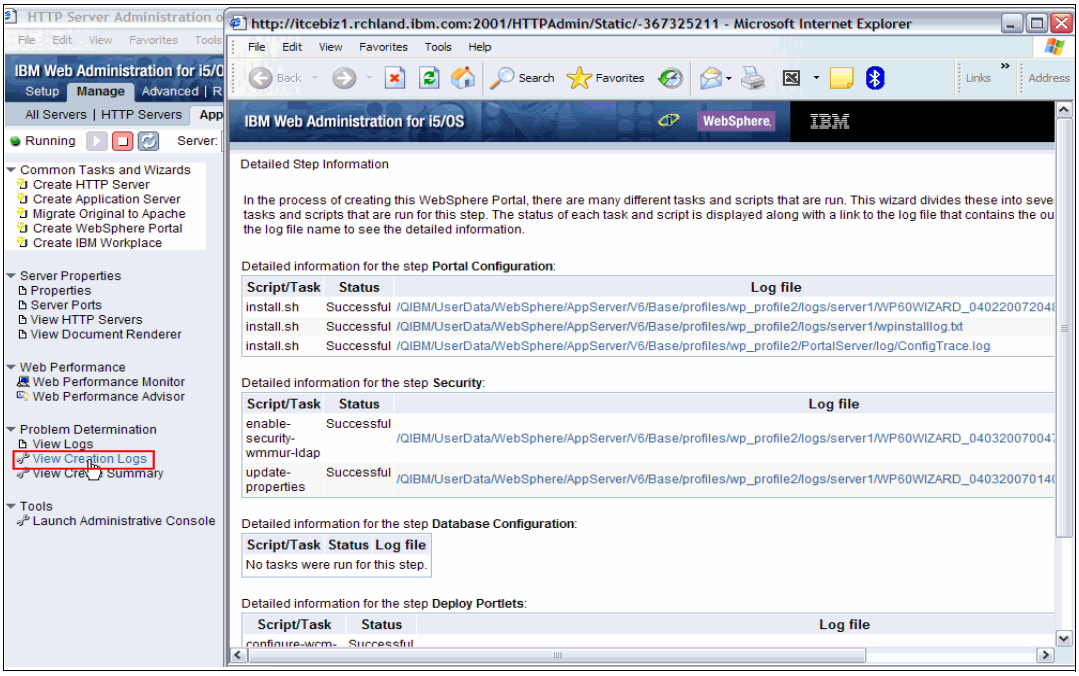

http://itcebiz1.rchland.ibm.com:2001/HTTPAdmin/Static/-367325211 - Microsoft Internet Explorer
IBM Web Administration for i5/OS
WebSphere
IBM
Detailed Step Information
Detailed information for the step Portal Configuration:
Detailed information for the step Security:
Detailed information for the step Database Configuration:
No tasks were run for this step.
Detailed information for the step Deploy Portlets:
View Creation Logs

Figure 3-55 Viewing the creation logs

It is a good practice to save the logs in the following directories after you configure a WebSphere Portal profile with IBM Web Administration for i5/OS:

- Save logs starting with `WP6OWIZARD_xxxxx_xxxxx.log` in directory: `/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<wp_profile>/logs/server1/WP6OWIZARD_xxxxxxxxx_xxxxxxxxx.log`
- `/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<wp_profile>/logs/server1/wpinstalllog.txt`
- `/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<wp_profile>/PortalServer/log/ConfigTrace.log`
- `/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<wp_profile>/logs/server1/wpinstalllog.txt`

Click **View Create Summary** to display the list of attributes used when the portal profile was configured (Figure 3-56 on page 90).

Tip: You *must* keep the file /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profile_name*>/logs/IBMWizPrintableSummary.html to access the creation summary documentation in the future.

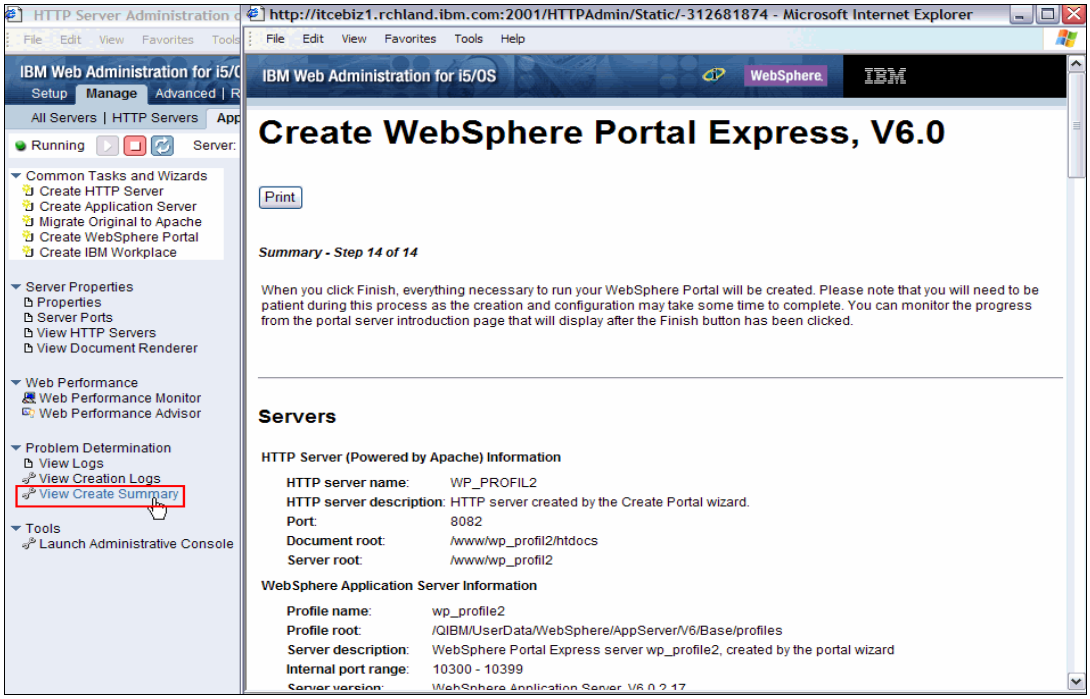

http://itcebiz1.rchland.ibm.com:2001/HTTPAdmin/Static/-312681874 - Microsoft Internet Explorer
IBM Web Administration for i5/OS
WebSphere
IBM
Create WebSphere Portal Express, V6.0
Print
Summary - Step 14 of 14
When you click Finish, everything necessary to run your WebSphere Portal will be created. Please note that you will need to be patient during this process as the creation and configuration may take some time to complete. You can monitor the progress from the portal server introduction page that will display after the Finish button has been clicked.
Servers
HTTP Server (Powered by Apache) Information
HTTP server name: WP_PROFIL2
HTTP server description: HTTP server created by the Create Portal wizard.
Port: 8082
Document root: /www/wp_profil2/htdocs
Server root: /www/wp_profil2
WebSphere Application Server Information
Profile name: wp_profile2
Profile root: /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles
Server description: WebSphere Portal Express server wp_profile2, created by the portal wizard
Internal port range: 10300 - 10399
Common Tasks and Wizards
Create HTTP Server
Create Application Server
Migrate Original to Apache
Create WebSphere Portal
Create IBM Workplace
Server Properties
Properties
Server Ports
View HTTP Servers
View Document Renderer
Web Performance
Web Performance Monitor
Web Performance Advisor
Problem Determination
View Logs
View Creation Logs
View Create Summary
Tools
Launch Administrative Console

Figure 3-56 Viewing the Create Summary

3.3 Understanding WebSphere Portal Express work management on i5/OS

This section provides an overview of the main libraries, directories, jobs, and user profiles associated with the configuration and runtime environment of WebSphere Portal Express.

3.3.1 WebSphere Portal Express product components on i5/OS

After you install WebSphere Portal Express on i5/OS, the following components are created:

- Product directory: /QIBM/ProdData/PortalExpress/V6. See Figure 3-57.

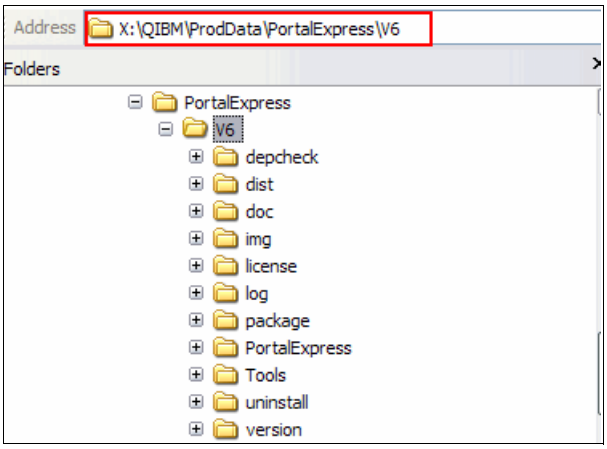


Figure 3-57 WebSphere Portal Express product data directory

- Product library: QWPE6001

After you configure a WebSphere Portal Express profile, the following components are created:

- WebSphere Portal Express profile:
  - User data directory:
    /QIBM/UserData/WebSphere/AppServer/V6/<*version*>/profiles/<*profile_name*>

    The version is BASE or ND, depending on the WebSphere Application Server version you selected when you configured the portal profile. See Figure 3-58.

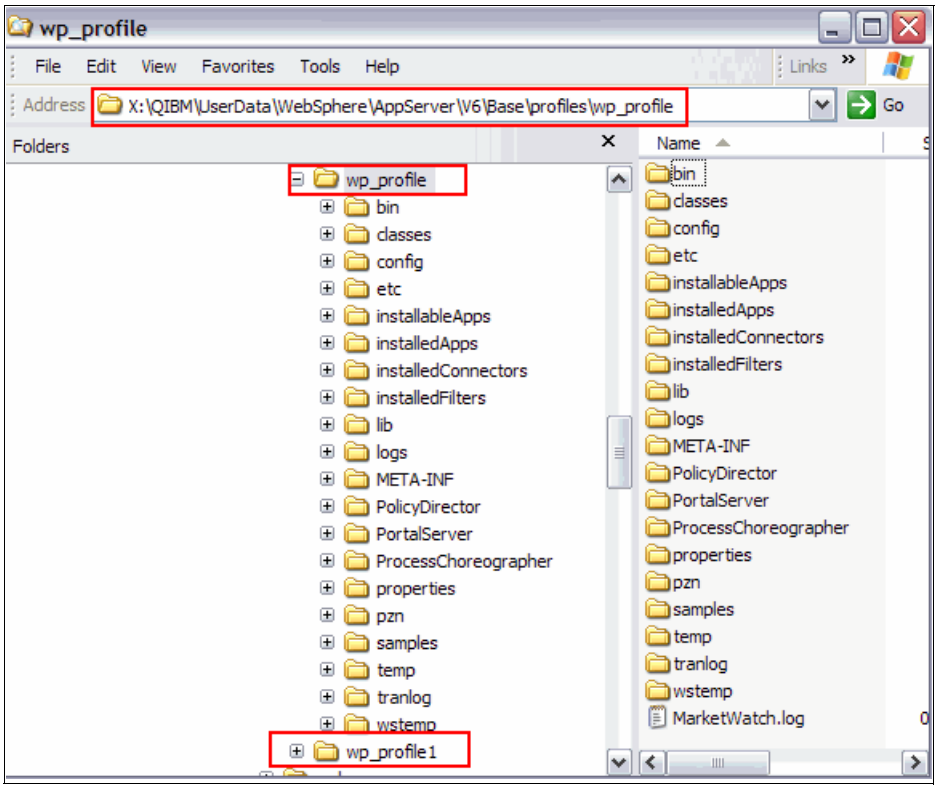


Figure 3-58 WebSphere Portal Express user data directory

  - The profile name is `wp_profile` for the first profile and `wp_profile`*X* for the subsequent profiles where *X* is an incremental number. You can alter the default naming convention by using the following command line arguments:

    Default: `wp_profile, wp_profile1, wp_profile2, ...`

    User-specified: `-W iSeriesdetectProfileAction.profileName=my_profile1`

    IBM Web Administration for i5/OS: The user can specify the desired value. It defaults to `wp_profile, wp_profile1, wp_profile2`, and so on.
  - Application servers: Two application servers are created for a portal profile. You only need to start WebSphere_Portal at run time:
    - server1: Admin application server
    - WebSphere_Portal: WebSphere Portal application server

– Port assignment: 50 consecutive ports are assigned to a portal profile. The first 25 ports are used for server1 and the remaining are for WebSphere_Portal.

  Default: Starting at 10000. Port conflicts are checked against started servers.

  User-specified: `-W iSeriesStartingPort.startingPort=12345`. Port conflicts are not checked.

  IBM Web Administration for i5/OS: The user can specify the desired value. It defaults to the first available port range, then checks for port conflicts against all configured WebSphere Application Server instances and profiles.

- Database owner user profile. This is the user profile that owns the portal databases:
  – wpdb2ins is for the first profile and wpdb2ins*X* is for the subsequent profiles where *X* is an incremental number.

    Default: `wpdb2ins, wpdb2ins1, wpdb2ins2, ...`

    User specified: `-W iSeriesDB2Database.user=mydb2ins`

    IBM Web Administration for i5/OS: The user can specify the desired value. It defaults to `wpsdb2ins, wpdb2ins1`, and so on.

    Note: The password for the database owner user profile is the same password specified for the portal administrator. The password *must* comply with your System i password rules.

- DB2 database schemes. Table 3-1 shows the default schema names (libraries) for the first WebSphere Portal Express profile created with WebSphere Application Server Base.

Table 3-1 Database purpose and default names for first portal profile created on WAS BASE

Description	Schema name
Community	WPECMM
Customer	WPECST
Feedback	WPEFDB
JCR	WPEJCR
LikeMinds	WPELKM
Release	WPEREL
WMM	<*DB user name*>, for example, wpdb2ins

The second profile configuration follows the same naming convention by adding a sequence number at the end of the name, for example, `WPECMM1`, `WPECSTS1`, and so on.

Table 3-2 on page 93 shows the default schema names (libraries) for the first WebSphere Portal Express profile created with WebSphere Application Server ND:

Table 3-2 Database purpose and default names for first portal profile created on WAS ND

Description	Schema name
Community	WPENCMM
Customer	WPENCST
Feedback	WPENFDB
JCR	WPENJCR
LikeMinds	WPENLKM
Release	WPENREL
WMM	<*DB user name*>, for example, wpdb2ins

– IBM Web Administration for i5/OS: Users can choose between naming databases based on their purpose as shown in Table 3-1 on page 92 or based on the profile name, for example, WP_PROFILE. Creation of portal profiles on WebSphere Application Server ND is not supported.

3.3.2 Identifying application servers associated with a portal profile

If you have more than one WebSphere Portal profile on your system, you have multiple WEBSPHERE_ jobs in the QWAS6 subsystem. You can determine which job goes with which profile by performing the following steps:

1. Display the jobs running in the QWAS6 subsystem. From a 5250 emulation session, enter the command `WRKACTJOB SBS(QWAS6)` and press Enter.
2. On the Work with Active Jobs display, enter option `5`, (Work with) by a WEBSPHERE_ job.
3. Type option `10` (Display job log) and note the portal profile name as shown in Figure 3-59.

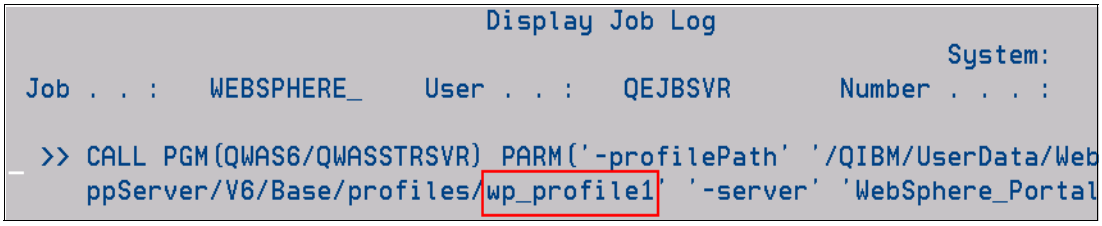

Display Job Log
System:
Job . . . : WEBSPHERE_ User . . . : QEJBSVR Number . . . :
>> CALL PGM(QWAS6/QWASSTRSVR) PARM('-profilePath' '/QIBM/UserData/Web
ppServer/V6/Base/profiles/wp_profile1' '-server' 'WebSphere_Portal

Figure 3-59 WEBSPHERE_ job associated with wp_profile1 portal profile

4. Ignore the error message shown in Figure 3-60 on page 94.

```
                              Display All Messages
                                                                System:   ITCEBIZ1
 Job . . :   WEBSPHERE_    User . . :   QEJBSVR       Number . . . :   226529

_ >> CALL PGM(QWAS6/QWASSTRSVR) PARM('-profilePath' '/QIBM/UserData/WebSphere/A
     ppServer/V6/Base/profiles/wp_profile5' '-server' 'WebSphere_Portal')
     ACGDTA for 226529/QEJBSVR/WEBSPHERE_ not journaled; reason 1.
     Java Virtual Machine is Classic.
     Server starting with user profile QEJBSVR and JDK 1.4.2.11.
     Job 226282/QUSER/QSQSRVR used for SQL server mode processing.
     Job 226603/QUSER/QSQSRVR used for SQL server mode processing.
     Job 226604/QUSER/QSQSRVR used for SQL server mode processing.
     Job 226606/QUSER/QSQSRVR used for SQL server mode processing.
     Job 226605/QUSER/QSQSRVR used for SQL server mode processing.
     Authorization failure on distributed database connection attempt.
     Job 226608/QUSER/QSQSRVR used for SQL server mode processing.
     Job 226607/QUSER/QSQSRVR used for SQL server mode processing.
     Job 226660/QUSER/QSQSRVR used for SQL server mode processing.
                                                                       Bottom
```

Figure 3-60 Ignoring the authorization failure on distributed database connection attempt message

3.3.3 Starting and stopping portal servers

The easiest way to start and stop portal servers is using IBM Web Administration for i5/OS. Perform the following steps:

1. Access the Web Administration for i5/OS. See 3.2.1, “Verifying the HTTP Administration server is active” on page 71 for details about how to access.
2. Select the WebSphere_Portal application server for your instance.
3. Click the red **Stop** icon (Figure 3-61).

Figure 3-61 Stopping a WebSphere_Portal application server instance

4. Select the portal components that you want to stop and click **Stop** (Figure 3-62).

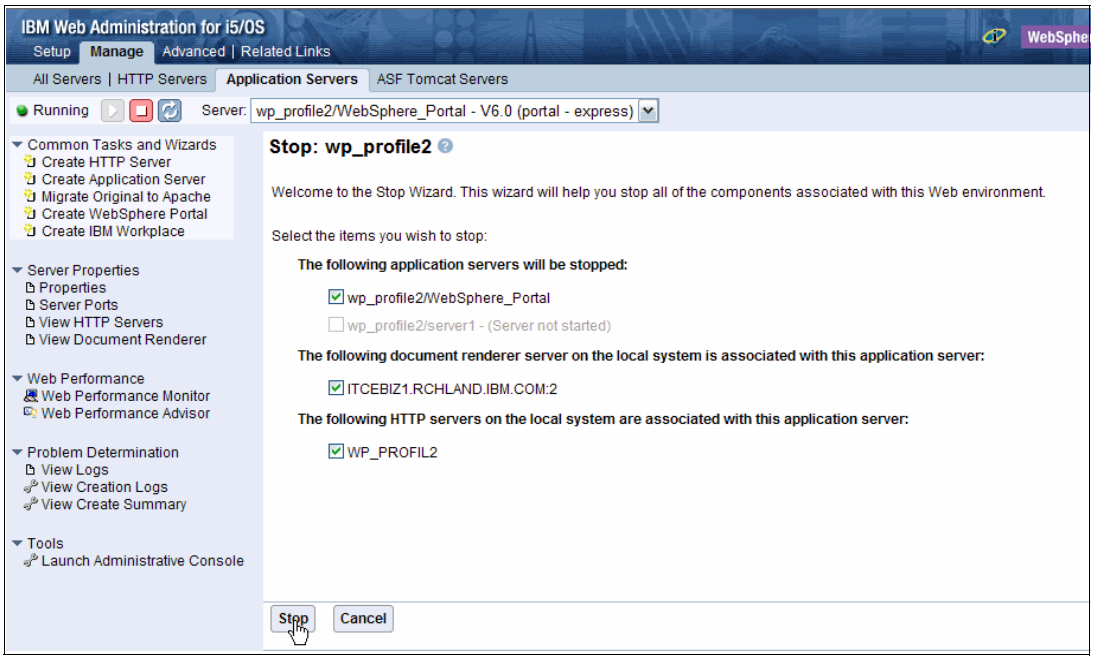


Figure 3-62 Stopping components associated with the portal environment

5. To start the servers for the portal profile, click the green **Start** icon (Figure 3-63).

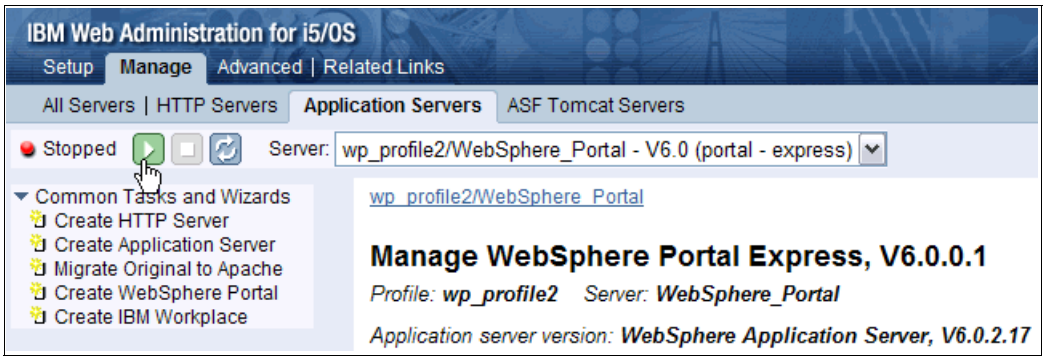


Figure 3-63 Starting the portal components

6. Select the servers you want to start and click **Start** (Figure 3-64).

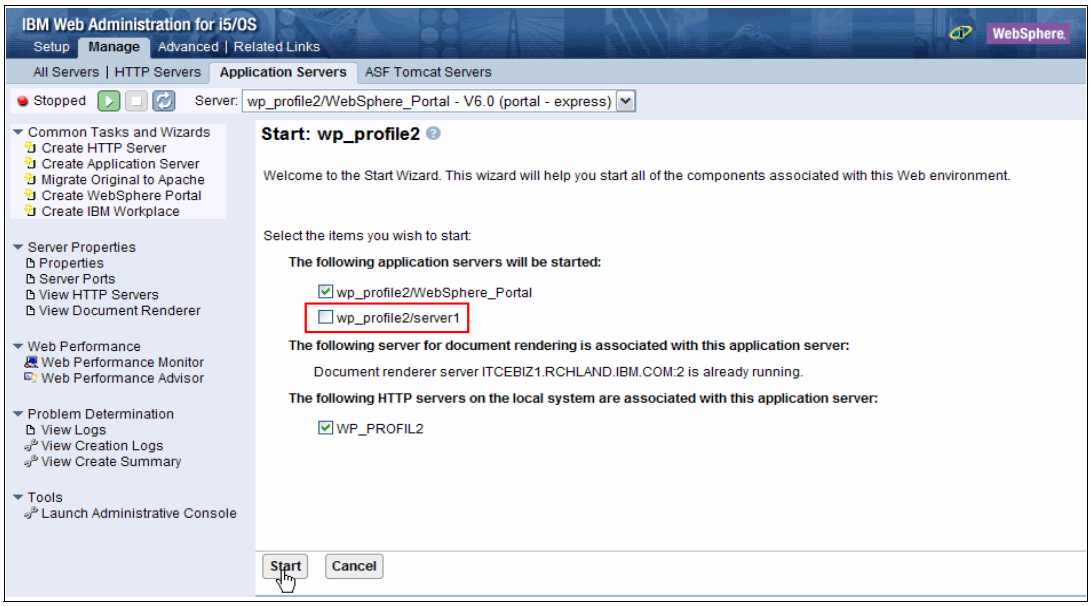


Figure 3-64 Starting the components associated with your portal environment

3.3.4 Starting portal servers when QWAS6 subsystem starts

Enter the following CL commands to start the portal servers when the QWAS6 subsystem starts:

1. `CRTLIB LIB(`*`WPDEMO`*`)` (Replace *WPDEMO* by a library name of your choice).
2. `CRTDUPOBJ OBJ(QWASJOBD) FROMLIB(QWAS6) OBJTYPE(*JOBD) TOLIB(WPDEMO) NEWOBJ(WPJOBD)`
3. `CHGJOBD JOBD(WPDEMO/WPJOBD) USER(QEJBSVR) RQSDTA('QSYS/CALL PGM(QWAS6/QWASSTRSVR) PARM(''-profilePath'' ''/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wp_profile1'' ''-server'' ''WebSphere_Portal'')')`
4. `ADDAJE SBSD(QWAS6/QWAS6) JOB(WEBSPHERE_) JOBD(WPDEMO/WPJOBD)`
5. `STRSBS SBSD(QWAS6/QWAS6)`

To start portal automatically at IPL, add `STRSBS SBSD(QWAS6/QWAS6)` to the program specified in the QSTRUPPGM system value.

3.4 Problem determination

This section includes information that you need to analyze WebSphere Portal Express installation and configuration problems or report problems to IBM. Perform the following steps when installation or configuration problems occur:

1. Check the status of the prerequisite PTFs and prerequisite WebSphere Application Server product as described in 2.6.1, “Required i5/OS V5R3 PTFs” on page 33, 2.6.2, “Required i5/OS V5R4 PTFs” on page 33, and 2.7.2, “Verifying the WebSphere Application Server environment” on page 37.

2. Check the WebSphere Portal Express installation logs and ConfigTrace.log. Refer to 3.4.1, “Installation log files” on page 97 for a complete list of installation log files.
3. Check the WebSphere Application Server log files at: `/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<wp_profile>/logs`
4. Check the LocalizeTrace.log file.

The ConfigTrace.log contains the following information:

- Configuration task that was run
- Property values associated with the task
- Outcome of the task: BUILD SUCCESSFUL or BUILD FAILED

To read the ConfigTrace.log file, start at the bottom and look for BUILD FAILED, then scroll up to see which task was the last one to run.

Tip: We recommend that you archive the configuration logs after the initial profile configuration and before you run the configuration tasks. Move the existing configuration logs to a log archive directory and restart the WebSphere_Portal server to generate the new configuration logs.

3.4.1 Installation log files

Installation logs are stored in the i5/OS integrated file system directory of /tmp/InstallShield. Table 3-3 lists the log files that are created during WebSphere Portal Express installation.

Table 3-3 WebSphere Portal Express installation log files

Log file name	Description	Problem symptoms
wpinstalllog.txt	Contains trace information that is generated by the installation program.	Check this log if the WebSphere Portal Express installation stops before successful completion.
wpinstalllog_base.txt	Contains a copy of wpinstalllog.txt before configuring.	Check this log if the WebSphere Portal Express configuration onto a WebSphere Application Server base profile stops before successful completion.
installmessages.txt	Contains messages that are generated during installation.	Check this log for errors generated during installation.
installtraces1.txt installtraces2.txt installtraces3.txt	Contains trace information generated by the dependency checking function. The output is added to installtraces1.txt until it reaches a predefined size, at which point output goes into installtraces2.txt and then into installtraces3.txt. When installtraces3.txt is full, the output reverts to installtraces1.txt and overwrites previous trace information.	Check these files if there are problems with component discovery and dependency checking.
iSeriesDB2Database.txt	Contains the names of the portal databases that were configured.	N/A

3.4.2 Configuration log files

Configuration logs are generated as a result of selecting the Install and Configure option of the installation program, or by running portal configuration tasks and installing fix packs. Configuration logs are stored in the portal profile directory of:

```
/QIBM/UserData/WebSphere/AppServer/V6/<version>/profiles/<wp_profile>/PortalServer/log
```

Tip: We recommend that you archive the configuration logs after the initial profile configuration and before you run the configuration tasks. Move the existing configuration logs to a log archive directory and restart the WebSphere Portal server to generate the new configuration logs.

Table 3-4 lists the WebSphere Portal Express configuration logs.

Table 3-4 WebSphere Portal Express configuration log files

Log file name	Description	Problem symptoms
LocalizeConfigTrace.log LocalizeConfigTrace1.log	Contains trace information about the create-all-db configuration task. The output is added to LocalizeConfigTrace.log until it reaches a predefined size, at which point the output goes into LocalizeConfigTrace1.log. When LocalizeConfigTrace1.log is full, the output reverts to LocalizeConfigTrace.log and overwrites previous trace information.	Check these logs if you have trouble creating databases.
LocalizeTrace.log	LocalizeTrace.log is a subset of LocalizeConfigTrace.log and contains actual commands entered.	Check this log for errors generated during installation.
ConfigTrace.log ConfigTrace1.log ConfigTraceMessages.log	Contains trace information about configuration tasks.	Check this log for errors during configuration tasks. Look for BUILD FAILED messages.
rstdb2schema.log	Contains information about the creation of the portal databases.	Check this log for errors in the portal database configuration.

The following localization log files are stored temporarily in the /tmp directory:

- /tmp/LocalizeTrace.log
- /tmp/LocalizeErr.log
- /tmp/LocalizeProgress.log

When the localization is completed, these logs are copied to this directory:

```
\QIBM\UserData\WebSphere\AppServer\V6\<version>\profiles\<wp_profile>\PortalServer\log
```

If the localization fails before the files are copied from the /tmp directory, look for the localization files in the temporary location.

3.4.3 WebSphere Portal Express version and history information

You can use the WebSphere Portal Express version information tool to gather information about the WebSphere Portal Express product. It provides a snapshot of the product

directories, installed components, and versions. Perform the following steps to run the Version Information tool:

1. From a 5250 session, enter the QSHELL environment, enter the CL command `STRQSH` and press Enter.
2. Enter the following command (replace *Base* with your WebSphere Application Server version and *wp_profile1* with your portal profile name):

   ```
   cd /qibm/userdata/websphere/appserver/v6/Base/profiles/wp_profile1/portalserver/bin
   ```

3. Enter the following command to direct the WPversion.sh output to a text file in the i5/OS integrated file system:

   ```
   WPversionInfo.sh | iconv -f 37 -t 819 > /tmp/wpversioninfo.txt
   ```

Figure 3-65 and Figure 3-66 on page 100 show the output of WPVersionInfo.sh.

```
WVER0010I: Copyright (c) IBM Corporation 2002; All rights reserved.
WVER0011I: WebSphere Portal
WVER0012I: VersionInfo reporter version 1.10.1.1, dated 7/29/05

--------------------------------------------------------------------------------
IBM WebSphere Portal Product Installation Status Report
--------------------------------------------------------------------------------

Report at date and time 2007-04-08T17:14:22-05:00

Installation
--------------------------------------------------------------------------------
Product Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wp_profile1/PortalServer
Version Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wp_profile1/PortalServer/ve
rsion
DTD Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wp_profile1/PortalServer/ve
rsion/dtd
Log Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wp_profile1/PortalServer/ve
rsion/log
Backup Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wp_profile1/PortalServer/ve
rsion/backup
TMP Directory       /tmp

Installation Platform
--------------------------------------------------------------------------------
Name           IBM WebSphere Portal
Version        6.0
```

Figure 3-65 WebSphere Portal Version Information tool output (1 of 2)

```
Technology List
--------------------------------------------------------------------------------
MP              installed
PDM             installed
WCM             installed
PZN             installed

Installed Product
--------------------------------------------------------------------------------
Name            IBM WebSphere Portal MultiPlatform
Version         6.0.0.1
ID              MP
Build Level     wp6001_073_03 2006-12-01
Build Date      12/01/2006

Installed Product
--------------------------------------------------------------------------------
Name            IBM WebSphere Portal Document Manager
Version         6.0.0.1
ID              PDM
Build Level     wp6001_080_01 2007-01-12
Build Date      01/12/2007

Installed Product
--------------------------------------------------------------------------------
Name            IBM WebSphere Portal Personalization
Version         6.0.0.1
ID              PZN
Build Level     wp6001_080_01 2007-01-12
Build Date      01/12/2007

Installed Product
--------------------------------------------------------------------------------
Name            IBM WebSphere WebSphere Portal Web Content Manager
Version         6.0.0.1
ID              WCM
Build Level     wp6001_080_01 2007-01-12
Build Date      01/12/2007
Installed Product
--------------------------------------------------------------------------------
Name            IBM WebSphere Portal MultiPlatform
Version         6.0.0.1
ID              MP
Build Level     wp6001_073
Build Date      12/01/2006
--------------------------------------------------------------------------------
End Installation Status Report
--------------------------------------------------------------------------------
```

Figure 3-66 WebSphere Portal Version Information tool output (2 of 2)

3.5 Deleting a WebSphere Portal Express profile

The easiest way to delete a portal profile is by using IBM Web Administration for i5/OS. Deleting a portal profile deletes the database user and portal libraries. Perform the following steps:

1. Access the Web Administration for i5/OS. See 3.2.1, “Verifying the HTTP Administration server is active” on page 71 for details about how to access.
2. From the Servers pull-down, select **All servers** (Figure 3-67).

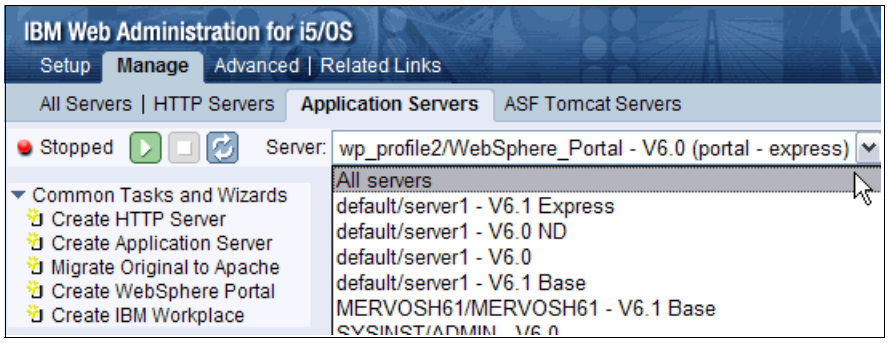


Figure 3-67 Selecting All servers

3. Select the server you want to delete. Make sure the server is stopped first. Click **Delete** (Figure 3-68).

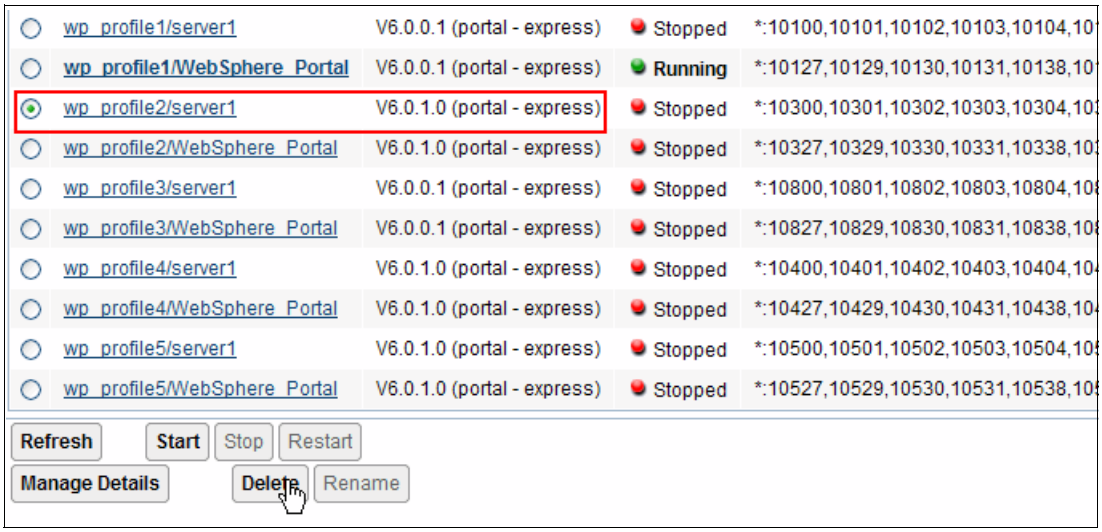

wp_profile1/server1 V6.0.0.1 (portal - express) Stopped
wp_profile1/WebSphere_Portal V6.0.0.1 (portal - express) Running
wp_profile2/server1 V6.0.1.0 (portal - express) Stopped
wp_profile2/WebSphere_Portal V6.0.1.0 (portal - express) Stopped
wp_profile3/server1 V6.0.0.1 (portal - express) Stopped
wp_profile3/WebSphere_Portal V6.0.0.1 (portal - express) Stopped
wp_profile4/server1 V6.0.1.0 (portal - express) Stopped
wp_profile4/WebSphere_Portal V6.0.1.0 (portal - express) Stopped
wp_profile5/server1 V6.0.1.0 (portal - express) Stopped
wp_profile5/WebSphere_Portal V6.0.1.0 (portal - express) Stopped
Refresh
Start
Stop
Restart
Manage Details
Delete
Rename

Figure 3-68 Selecting the portal server to delete

4. The DB2 database owner and portal libraries are deleted with the portal profile (Figure 3-69). Click **Next**.

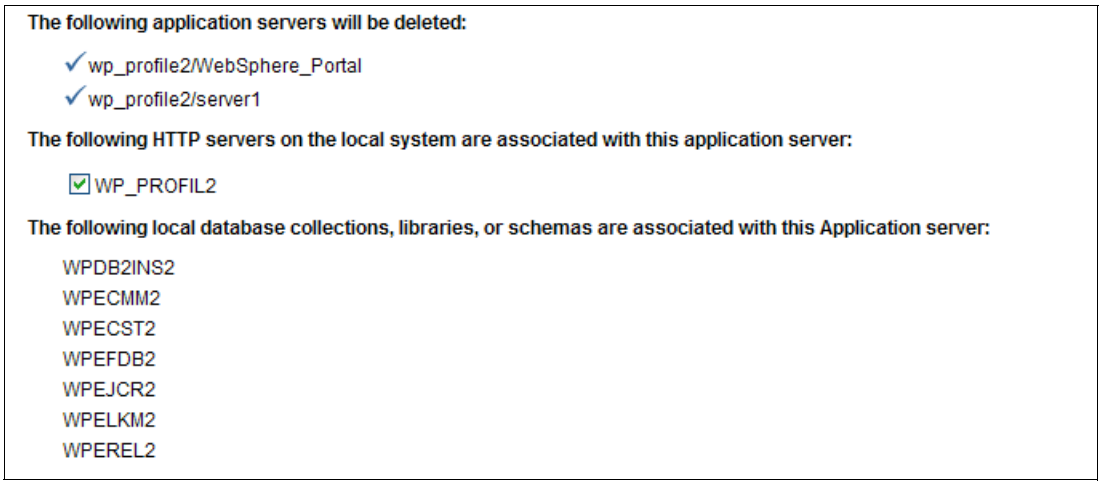


Figure 3-69 WebSphere Portal profile items to delete

5. On the Summary page, click **Delete**. See Figure 3-70.

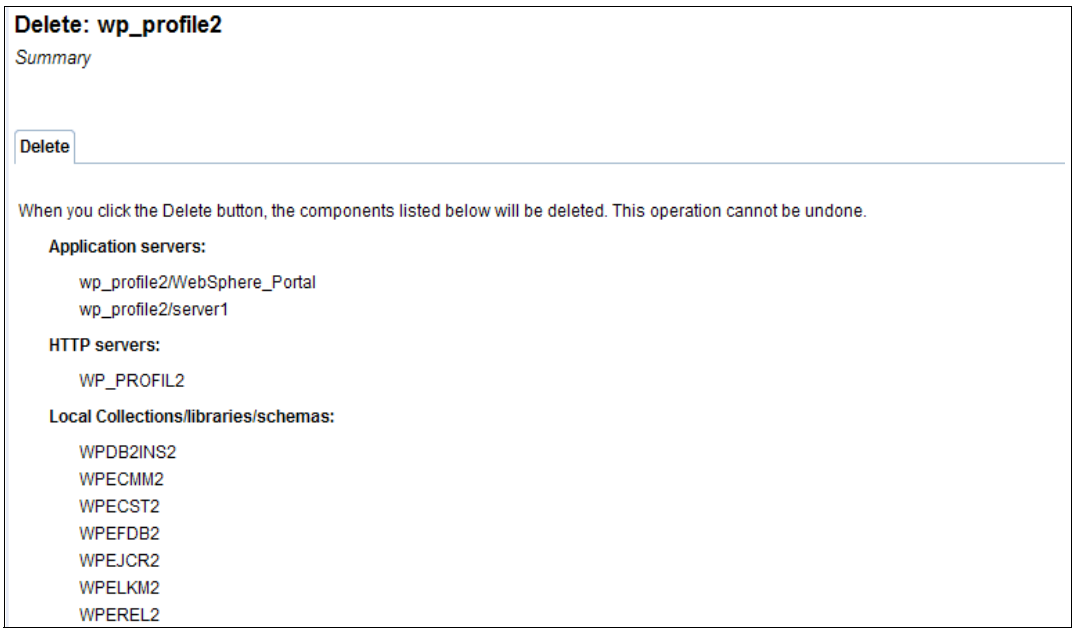


Figure 3-70 Confirming that you want to delete the portal profile, HTTP server, and libraries

6. To refresh the window, click **Refresh**. See Figure 3-71.

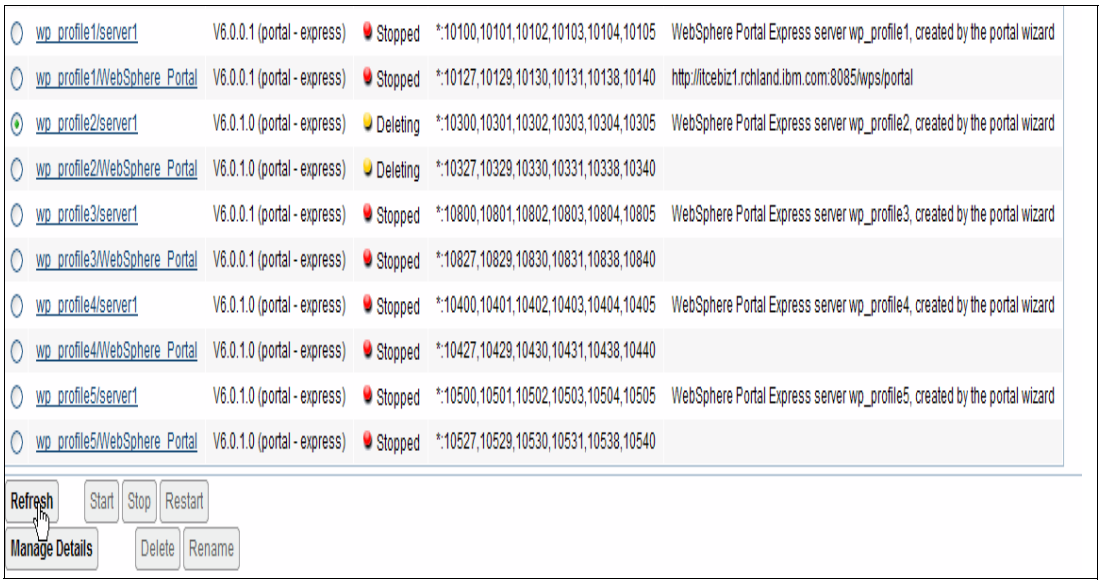

wp_profile1/server1 V6.0.0.1 (portal - express) Stopped *:10100,10101,10102,10103,10104,10105 WebSphere Portal Express server wp_profile1, created by the portal wizard
wp_profile1/WebSphere_Portal V6.0.0.1 (portal - express) Stopped *:10127,10129,10130,10131,10138,10140 http://itcebiz1.rchland.ibm.com:8085/wps/portal
wp_profile2/server1 V6.0.1.0 (portal - express) Deleting *:10300,10301,10302,10303,10304,10305 WebSphere Portal Express server wp_profile2, created by the portal wizard
wp_profile2/WebSphere_Portal V6.0.1.0 (portal - express) Deleting *:10327,10329,10330,10331,10338,10340
wp_profile3/server1 V6.0.0.1 (portal - express) Stopped *:10800,10801,10802,10803,10804,10805 WebSphere Portal Express server wp_profile3, created by the portal wizard
wp_profile3/WebSphere_Portal V6.0.0.1 (portal - express) Stopped *:10827,10829,10830,10831,10838,10840
wp_profile4/server1 V6.0.1.0 (portal - express) Stopped *:10400,10401,10402,10403,10404,10405 WebSphere Portal Express server wp_profile4, created by the portal wizard
wp_profile4/WebSphere_Portal V6.0.1.0 (portal - express) Stopped *:10427,10429,10430,10431,10438,10440
wp_profile5/server1 V6.0.1.0 (portal - express) Stopped *:10500,10501,10502,10503,10504,10505 WebSphere Portal Express server wp_profile5, created by the portal wizard
wp_profile5/WebSphere_Portal V6.0.1.0 (portal - express) Stopped *:10527,10529,10530,10531,10538,10540
Refresh
Start
Stop
Restart
Manage Details
Delete
Rename

Figure 3-71 Deleting a portal profile

3.6 Uninstalling the WebSphere Portal Express product

You *must* remove all WebSphere Portal profiles before uninstalling WebSphere Portal Express. Refer to WebSphere Portal Express Information Center for information about uninstalling portal on i5/OS at:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/topic/com.ibm.wp.ent.doc/wpf/is_uni.html

4

Initial performance tuning

This chapter describes the initial tuning that enhances the performance of your WebSphere Portal Express environment running on i5/OS. The first part of the chapter describes the Web Performance Advisor tool, which tunes the environment (system, Web application server, and HTTP server). The following sections list the individual parameters that you can tune (several of the parameters are covered by the Web Performance Advisor tool). This list is intended to be used only for an initial tuning. Monitor the runtime environment and adjust the settings appropriately based on your specific environment.

Note: If you modify individual parameters, we recommend that you check the Web Performance Advisor tool to make sure that the modification you made did not alter other settings.

© Copyright IBM Corp. 2007. All rights reserved.

4.1 Web Performance Advisor

The Web Performance Advisor tool monitors, evaluates, and modifies the performance attributes of your Web environment. A *Web environment* is a grouping of related Web and application servers that form a Web solution. A Web environment is made up of a single WebSphere Application Server instance or profile. The instance or profile can include many application servers. Each server has its own set of attributes that needs to be evaluated and adjusted. The Web environment also includes any associated HTTP servers and system attributes that can have a direct impact on performance. Each component of the Web environment contains attributes that can affect the overall performance of this environment.

4.1.1 Prerequisites

Support for the Web Performance Advisor tool was added to the IBM HTTP Server for i5/OS (5722-DG1) program product and was made available with the following group PTFs:

- For V5R3: PTF Group SF99099 level 14 or later
- For V5R4: PTF Group SF99114 level 8 or later

You access the Web Performance Advisor tool by using the Web Administration for i5/OS interface. The following Web browsers are supported:

- Microsoft Internet Explorer V6.*x*
- Mozilla FireFox V1.5.*x*

The Web Performance Advisor feature supports a variety of WebSphere-based products. These include WebSphere Application Server, WebSphere Portal Server, and IBM Workplace. Another supported product is IBM HTTP Server (powered by Apache) when the HTTP server is configured by one of the previously listed products.

For Web Performance Advisor to fully support WebSphere Portal Express V6, WebSphere Application Server V6.0.2.17 or higher is required.

4.1.2 Accessing the Web Performance Advisor

Because Web Performance Advisor is part of the Web Administration for i5/OS interface, you *must* start the *ADMIN instance of the HTTP server. Perform the following steps to access the Web Performance Advisor:

1. Start a Web browser and type in the URL:

   `http://your_system:2001/HTTPAdmin`

2. From the IBM Web Administration for i5/OS interface, select the server you want to examine. In the left navigation pane, select **Web Performance** → **Web Performance Advisor** (Figure 4-1).

> **Note:** If Web Performance Advisor is not displayed in the navigation pane, either the correct level of PTF Group SF99114 has not been properly installed, or the selected server is not supported by the Web Performance Advisor tool.

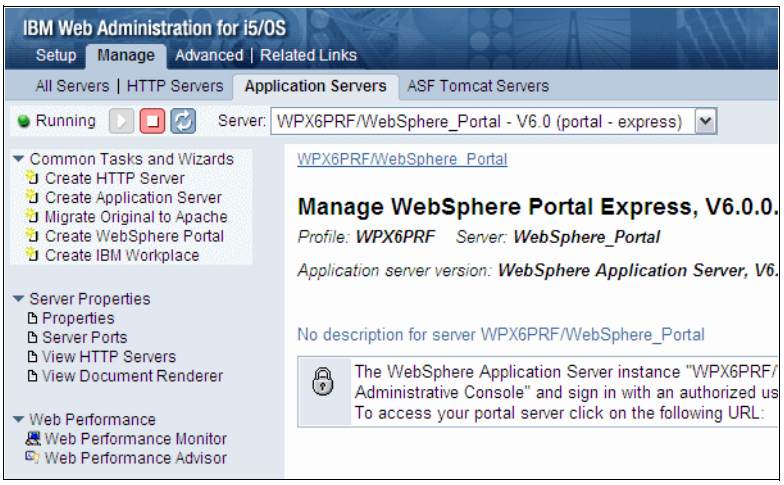


Figure 4-1 Accessing the Web Performance Advisor

3. The Web Performance Advisor interface displays two sets of performance attributes, system attributes, and Web environment attributes. Web environment attributes include both the Web server and the application servers, which are `WebSphere_Portal` and `server1` in our example (Figure 4-2).

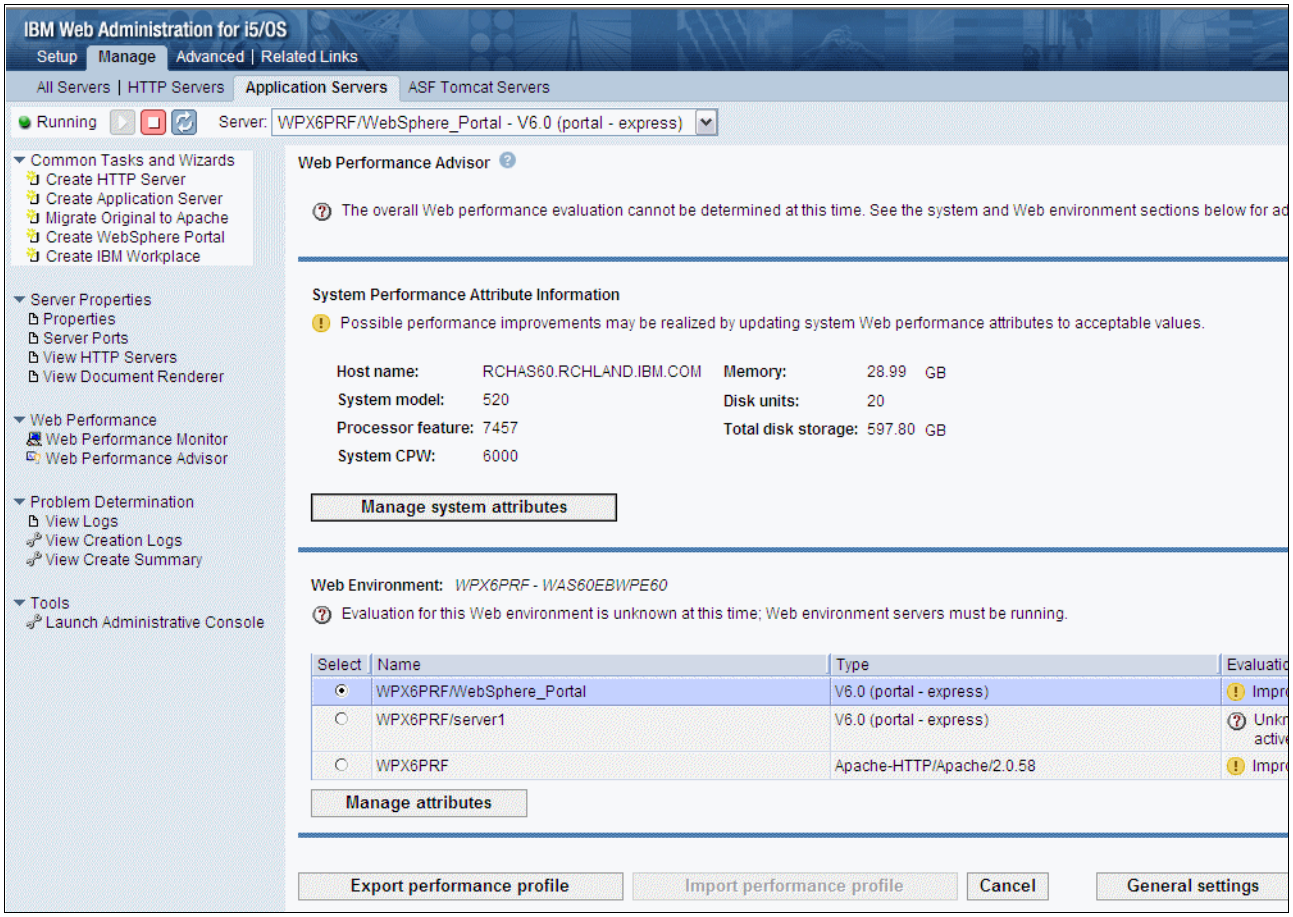


Figure 4-2 Web Performance Advisor interface

4.1.3 System attributes

By clicking **Manage system attributes** in Figure 4-2 on page 108, you can assess the system resources and the system performance settings. You can also check whether the proper PTFs are applied. See Figure 4-3.

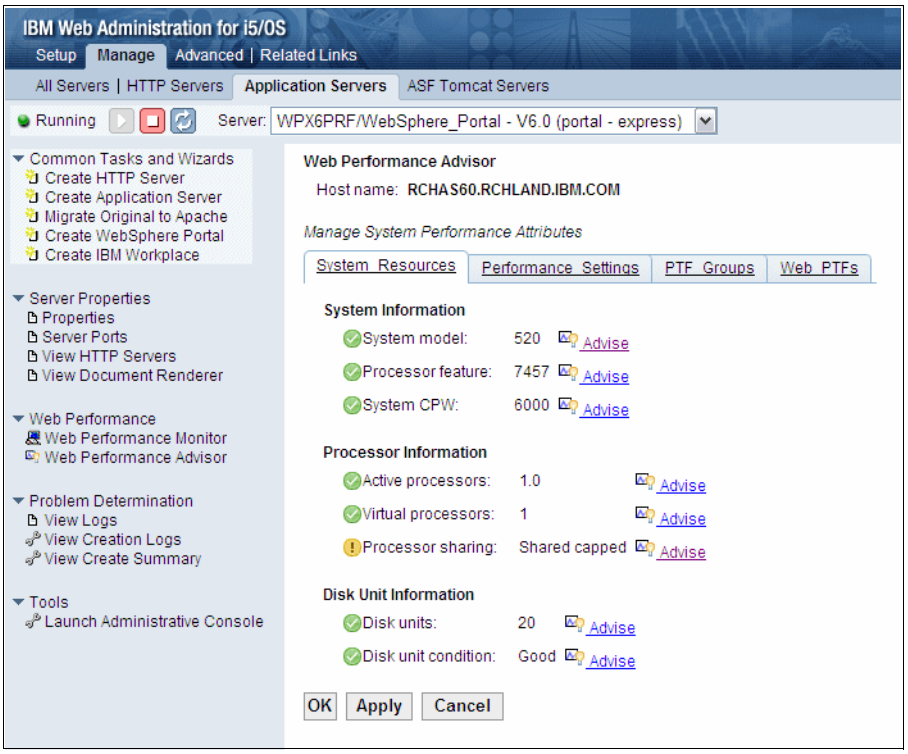


Figure 4-3 Web Performance Advisor: Manage System Performance Attributes, System Resources tab

Table 4-1 shows the system resources and their recommended values.

Table 4-1 System resources and their recommended values

Resource	Web Performance Advisor recommendation	Reference
System model	Use Workload Estimator	2.1, “Sizing the system” on page 16
Processor feature	Use Workload Estimator	2.1, “Sizing the system” on page 16
System CPW	Use Workload Estimator	2.1, “Sizing the system” on page 16
Active processors	1.0	4.5.1, “Processors” on page 126
Virtual processors	1	4.5.1, “Processors” on page 126
Processor sharing	Shared uncapped	4.5.1, “Processors” on page 126
Disk units	Use Workload Estimator	2.1, “Sizing the system” on page 16
Disk unit condition	Good	4.5.2, “Direct Access Storage Devices” on page 126

Table 4-2 shows the performance settings and their recommended values.

Table 4-2 Performance settings and their recommended values

Resource	Web Performance Advisor recommendation	Reference
Processor multitasking	Enabled	4.2.1, “Processor multitasking: QPRCMLTTSK” on page 115
Parallel processing degree	Optimize or None	4.2.5, “Parallel processing degree: QQRYDEGREE” on page 118
Thread resources adjustment	Enabled	4.2.6, “Thread resource adjustment: QTHDRSCADJ” on page 119
Performance adjustment	No adjustment	4.2.3, “Performance adjustment: QPFRADJ” on page 116
Thread resource affinity group	No group	4.2.7, “Thread resource affinity: QTHDRSCAFN” on page 119
Thread resource affinity level	Best available resource	4.2.7, “Thread resource affinity: QTHDRSCAFN” on page 119
Maximum activity level of system	No maximum	4.2.2, “Maximum activity level of system: QMAXACTLVL” on page 116
TCP/IP send buffer size	65535 Bytes	4.6.4, “Send and receive buffer sizes” on page 130
TCP/IP receive buffer size	65535 Bytes	4.6.4, “Send and receive buffer sizes” on page 130

4.1.4 Web Environment attributes

By selecting your HTTP server and clicking **Manage attributes** in the Web Environment section in Figure 4-2 on page 108, you can assess the HTTP server performance attributes shown in Figure 4-4 on page 111.

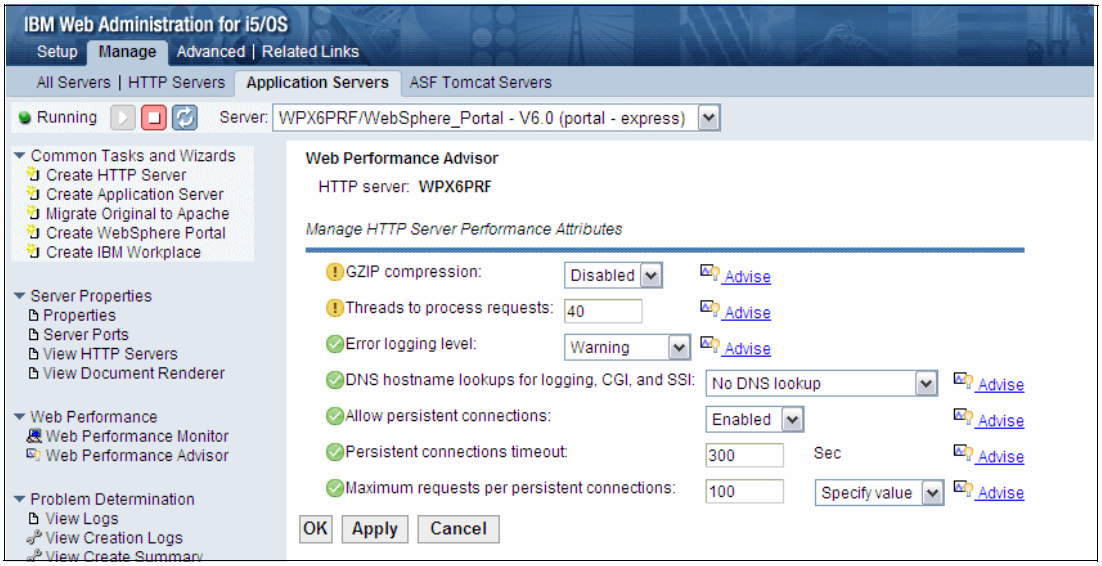


Figure 4-4 Web Performance Advisor: Web environment attributes for the Web server

Table 4-3 shows the parameters that you can tune using Web Performance Advisor and the recommended values.

Table 4-3 Web server attributes and the recommended values

Resource	Web Performance Advisor recommendation	Reference
GZIP compression	Enabled	4.7.1, “Traffic compression” on page 130
Threads to process requests	55	4.7.2, “General server configuration” on page 131
Error logging level	Warning	4.7.4, “Logging levels” on page 134
DNS host name lookup for logging, CGI, and SSI	No DNS lookup	4.7.2, “General server configuration” on page 131
Allow persistent connections	Enabled	4.7.3, “HTTP connections” on page 133
Persistent connections timeout	300	4.7.3, “HTTP connections” on page 133
Maximum requests per persistent connection	No maximum	4.7.3, “HTTP connections” on page 133

By selecting your WebSphere Application Server and clicking **Manage attributes** in the Web Environment section in Figure 4-2 on page 108, you are able to assess the JVM settings, the Web resources, the JDBC™ resources, and additional settings shown in Figure 4-5 on page 112.

Note: If the level of your WebSphere Application Server is V6.0.2.19 or higher, the JDBC Resources tab displays the resources at the server, node, and cell level. If the level of your WebSphere Application Server is lower than V6.0.2.19, then the JDBC Resources tab displays only the resources at the server and node level.

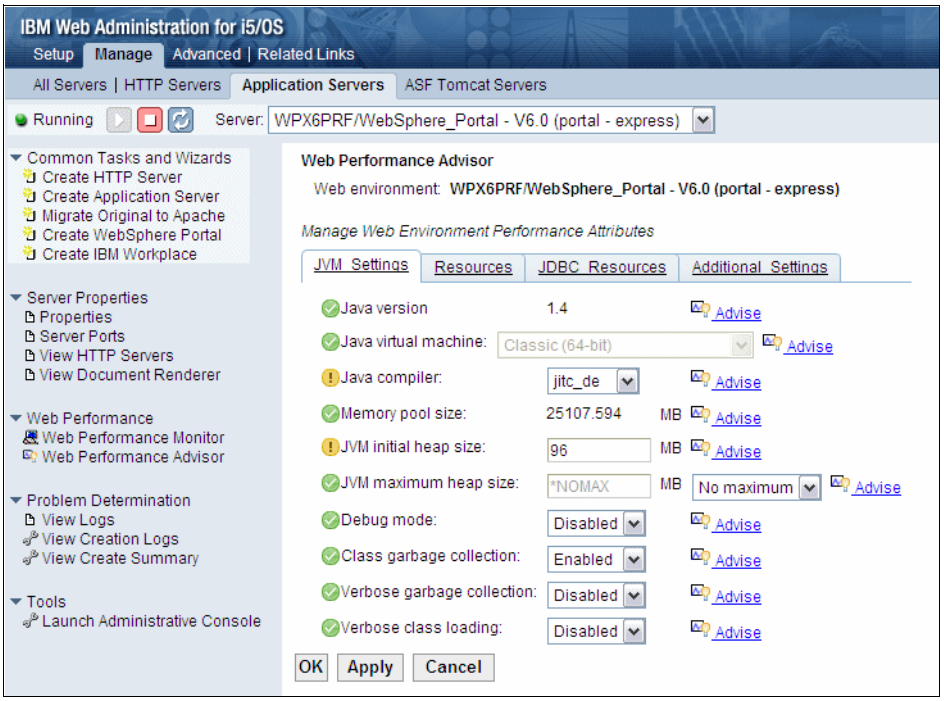


Figure 4-5 Web Performance Advisor: Web environment attributes for the WebSphere Application Server

Table 4-4 shows the JVM settings and their recommended values.

Table 4-4 JVM settings and their recommended values

Resource	Web Performance Advisor recommendation	Reference
Java compiler	jitc	4.8.2, “Java Virtual Machine” on page 137
Memory pool size	4 GB minimum, to be adjusted with performance testing	4.3.2, “Memory pool size” on page 122
JVM initial heap size	256 MB	4.8.2, “Java Virtual Machine” on page 137
JVM maximum heap size	No maximum	4.8.2, “Java Virtual Machine” on page 137
Debug mode	Disabled	N/A
Class garbage collection	Enabled	4.8.2, “Java Virtual Machine” on page 137
Verbose garbage collection	Disabled	4.8.2, “Java Virtual Machine” on page 137
Verbose class loading	Disabled	N/A

Table 4-5 show the WebSphere Application Server resources and their recommended values.

Table 4-5 WebSphere Application Server resources and their recommended values

Resource	Web Performance Advisor recommendation	Reference
Environment per memory pool	Single	4.3.1, “Running WebSphere Portal in a dedicated memory pool” on page 121
Maximum active	3590	4.3.3, “Memory pool activity level” on page 123
Web container minimum threads	70	4.8.4, “Servlet engine thread pool” on page 144
Web container maximum threads	70	4.8.4, “Servlet engine thread pool” on page 144
Process priority	20	N/A
Maximum sessions in memory	1000	N/A
Session timeout	30 minutes	4.8.5, “Session timeout” on page 147

Table 4-6 shows WebSphere Application Server additional settings and their recommended values.

Table 4-6 WebSphere Application Server additional settings and their recommended values

Resource	Web Performance Advisor recommendation	Reference
ESI caching	Enabled	4.8.3, “Caching” on page 142
WebSphere PMI	Enabled	N/A
WebSphere JVMPI	Disabled	N/A
Keep alive	Enabled	4.7.3, “HTTP connections” on page 133
WebSphere tracing	Informational	4.8.6, “Logging level” on page 148

4.1.5 Adjusting parameters

In case a parameter needs adjustment, the Web Performance Advisor advises you about what you need to do. Click **Advise** for the parameter that needs to be adjusted. A pop-up window appears with a recommended value for that parameter. See Figure 4-6 on page 114.

Note: Web Performance Advisor recommendations might be higher than the minimum requirements, based on the overall environment settings.

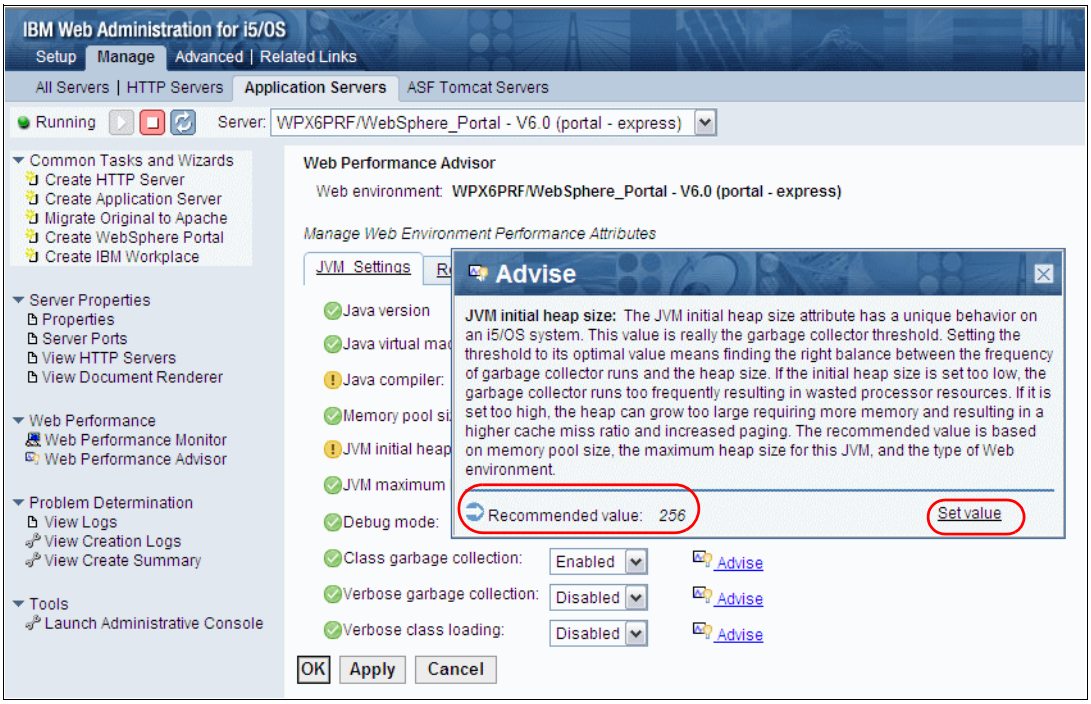

IBM Web Administration for i5/OS
Setup
Manage
Advanced | Related Links
All Servers | HTTP Servers
Application Servers
ASF Tomcat Servers
Running
Server: WPX6PRF/WebSphere_Portal - V6.0 (portal - express)
Common Tasks and Wizards
Create HTTP Server
Create Application Server
Migrate Original to Apache
Create WebSphere Portal
Create IBM Workplace
Server Properties
Properties
Server Ports
View HTTP Servers
View Document Renderer
Web Performance
Web Performance Monitor
Web Performance Advisor
Problem Determination
View Logs
View Creation Logs
View Create Summary
Tools
Launch Administrative Console
Web Performance Advisor
Web environment: WPX6PRF/WebSphere_Portal - V6.0 (portal - express)
Manage Web Environment Performance Attributes
JVM Settings
Advise
JVM initial heap size: The JVM initial heap size attribute has a unique behavior on an i5/OS system. This value is really the garbage collector threshold. Setting the threshold to its optimal value means finding the right balance between the frequency of garbage collector runs and the heap size. If the initial heap size is set too low, the garbage collector runs too frequently resulting in wasted processor resources. If it is set too high, the heap can grow too large requiring more memory and resulting in a higher cache miss ratio and increased paging. The recommended value is based on memory pool size, the maximum heap size for this JVM, and the type of Web environment.
Recommended value: 256
Set value
Java version
Java compiler:
Memory pool si
JVM initial heap
JVM maximum
Debug mode:
Class garbage collection: Enabled
Verbose garbage collection: Disabled
Verbose class loading: Disabled
Advise
OK
Apply
Cancel

Figure 4-6 Web Performance Advisor advice for processor settings

To apply the recommendations from the Web Performance Advisor interface, click **Set value** and then click **Apply** to activate it. Web Performance Advisor saves all of the values before applying the changes, then applies the changes and saves the new configuration. This allows you to go back to the original state if the new settings appear to be causing problems.

All configuration files are saved in the i5/OS integrated file system directory of /QIBM/UserData/HTTPA/admin/WPA. The Web Performance Advisor tool does not remove these files. We recommend that you back up these files before removing them. This allows you to keep track of every change made using Web Performance Advisor to the portal configuration.

Note: In a few cases, Web Performance Advisor only advises you about the recommended value, but it does not allow you to set the value through its interface. In that case, you need to manually apply the Web Performance Advisor recommendation. For example, this is the case for the system processor settings, and in this particular case, you need to use your Hardware Management Console (HMC).

4.1.6 Additional tuning parameters

Additionally, in Table 4-7 on page 115 we show more tuning parameters that are not covered by the Web Performance Advisor.

Table 4-7 Additional tuning parameters not covered by the Web Performance Advisor

Resource	Recommendation	Reference
Machine storage pool size	Faulting rate < 10 per second	4.2.4, “Machine storage pool size: QMCHPOOL” on page 117
Memory pool expert cache	*CALC	4.3.4, “Memory pool expert cache” on page 124
TCP/IP line speed and duplex support	Automatic	4.6.1, “Line speed and duplex support” on page 128
TCP/IP maximum frame size	1496 if line speed < 1 GB 8896 if line speed = 1 GB	4.6.2, “Maximum frame size” on page 128
TCP/IP Maximum Transmission Unit	Line description	4.6.3, “Maximum transmission unit” on page 128
Default application server (server1)	Stopped for normal operations	4.8.1, “Default application server” on page 137
Database jobs	Dedicated memory pool	4.9, “Database” on page 150

4.2 System tuning

This section describes the i5/OS system values that you can adjust to enhance WebSphere Portal Express performance.

4.2.1 Processor multitasking: QPRCMLTTSK

This system value sets the multitasking capability of the system to be on, off, or system-controlled. When enabled, each processor is concurrently executing multiple tasks at the same time. Using this value increases the performance capacity of the system or improves the responsiveness of a multi-threaded application.

A change to this system value takes effect at the next IPL.

The possible values are:

- 0 = Off
- 1 = On
- 2 = System-controlled

The recommended value is either 1 (On) or 2 (System-controlled).

To set the required value, use the following i5/OS CL command:

```
CHGSYSVAL SYSVAL(QPRCMLTTSK) VALUE('1')
```

Note: The default setting of the i5/OS system value QPRCMLTTSK might be incorrect for some V5R3M0 installations. See APAR II13981 at the following Web site:

http://www-912.ibm.com/n_dir/nas4apar.nsf/0/a4eaa9d8cb2ab5dd86256f690056c078?OpenDocument

4.2.2 Maximum activity level of system: QMAXACTLVL

This system value controls the number of threads that can compete at the same time for main storage and processor resources. For all active subsystems, the sum of all the threads running in all storage pools cannot exceed this value. If a thread cannot be processed because the maximum activity level has been reached, the thread is held until another thread reaches a time slice end or a long wait.

A change to this system value takes effect immediately.

The possible values are:

- From 2 to 32767
- *NOMAX

The recommended value is *NOMAX.

To set the required value, use the following i5/OS command:

```
CHGSYSVAL SYSVAL(QMAXACTLVL) VALUE(*NOMAX)
```

Or from the iSeries Navigator, select ***your system*** → **Configuration and Service** → **System Values** → **Performance** → **Memory Pools** (Figure 4-7).

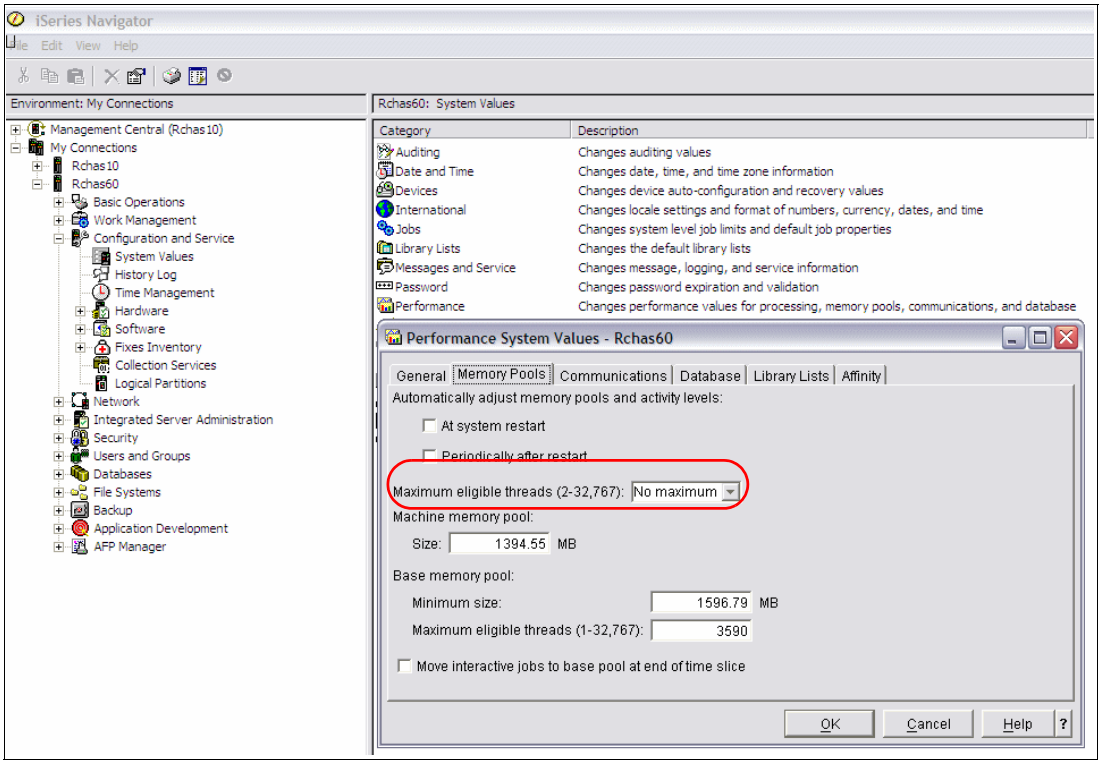


Figure 4-7 Setting system value QMAXACTLVL

4.2.3 Performance adjustment: QPFRADJ

This system value specifies whether the system needs to adjust values during IPL, at regular intervals for system pool sizes and activity levels, or both.

A change to this system value takes effect immediately.

The possible values are:

- 0 = No adjustment
- 1 = Adjustment at IPL
- 2 = Adjustment at IPL and automatic adjustment
- 3 = Automatic adjustment

The recommended value is 3 (Automatic adjustment) at installation and configuration time to determine the initial pool size. After WebSphere Portal is installed, configured, and up and running, set this value to 0 (No adjustment) to prevent other memory pools from stealing memory from the pool where the portal instance is running in *BASE by default. Periodically monitor the faulting rates and make manual adjustments to the memory pool.

Note: If you manually tune the performance of your machine, changing this system value to adjust performance values automatically causes you to lose your manual settings.

To set the required value, use the following i5/OS command:

```
CHGSYSVAL SYSVAL(QPFRADJ) VALUE('0')
```

Or from the iSeries Navigator, select ***your system*** → **Configuration and Service** → **System Values** → **Performance** → **Memory Pools** (Figure 4-8).

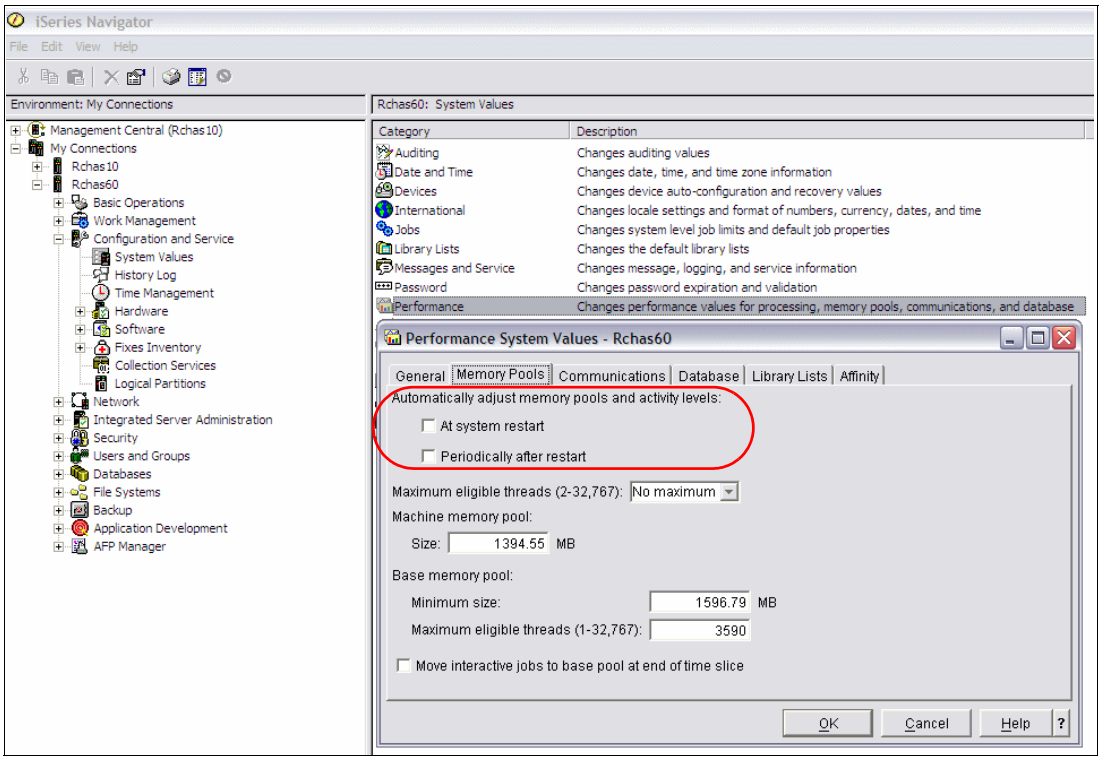


Figure 4-8 Setting system value QPFRADJ

4.2.4 Machine storage pool size: QMCHPOOL

This system value sets the size of the machine storage pool, which contains the highly shared machine and operating system licensed programs. You *must* be careful when changing this

value, because system performance might be impaired if the storage pool is too small. A change to this system value takes effect immediately.

The possible values range from 256 to 2147483647 KB.

A good guideline is for this value to be two times the machine pool “reserved size.” If the faulting rate exceeds 10 faults per seconds, then add more memory to System pool 1.

Note: The performance adjustment function can change the value when the system value QPFRADJ is set to either 1, 2, or 3.

To set the required value, use the following i5/OS command, where *xxxx* is the appropriate value for your system:

```
CHGSYSVAL SYSVAL(QMCHPOOL) VALUE('xxxx')
```

Or from the iSeries Navigator, select ***your system*** → **Configuration and Service** → **System Values** → **Performance** → **Memory Pools** (Figure 4-9).

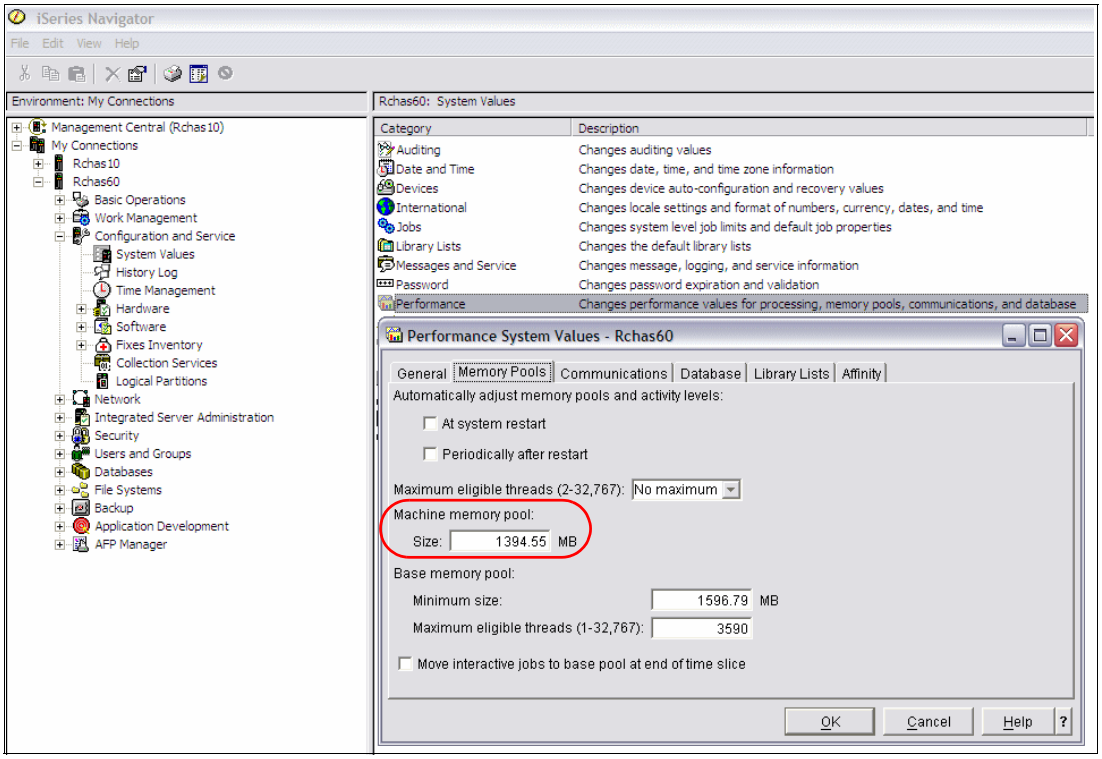


Figure 4-9 Setting system value QMCHPOOL

4.2.5 Parallel processing degree: QQRYDEGREE

This system value controls the parallel processing option and the type of parallel processing that are allowed.

The possible values are:

- *NONE = No parallel processing.
- *IO = Any number of tasks might be used when the database query optimizer chooses to use I/O parallel processing. No symmetric multiprocessor (SMP) parallel processing.

- *OPTIMIZE = The query optimizer can choose to use any number of tasks for either I/O or SMP parallel processing.
- *MAX = The query optimizer can choose to use either I/O or SMP parallel processing.

The recommend value is either *NONE or *OPTIMIZE.

To set the require value, use the following i5/OS command:

```
CHGSYSVAL SYSVAL(QQRYDEGREE) VALUE('xxxx')
```

4.2.6 Thread resource adjustment: QTHDRSCADJ

This system value specifies whether or not the system needs to make adjustments to the affinity of threads currently running in the system.

The possible values are:

- 0 = No adjustment
- 1 = Dynamic adjustment

The recommend value is 0 (No adjustment).

To set the require value, use the following i5/OS command:

```
CHGSYSVAL SYSVAL(QTHDRSCADJ) VALUE('0')
```

4.2.7 Thread resource affinity: QTHDRSCAFN

This system value specifies whether or not secondary threads have an affinity to the same group of processors and memory as the initial thread.

For the affinity group, the possible values are:

- *GROUP = Threads have affinity to the same group of processors and memory as the initial thread.
- *NOGROUP = Threads are not grouped together with the initial thread.

The recommend value is *NOGROUP.

For the affinity level, the possible values are:

- *NORMAL = Threads will use any processor or memory in the system if the resources they have affinity with are unavailable.
- *HIGH = Threads will only use resources with which they have affinity.

The recommend value is *NORMAL.

To set the require values, type the following i5/OS command and press F4 to prompt the command:

```
CHGSYSVAL SYSVAL(QTHDRSCAFN)
```

Enter the required values as shown in Figure 4-10 on page 120.

```
                              Change System Value

 System value . . . . . :   QTHDRSCAFN
 Description  . . . . . :   Thread resources affinity

Type choices, press Enter.

   Thread resources affinity:
     Group  . . . . . .   *NOGROUP       *NOGROUP, *GROUP
     Level  . . . . . .   *NORMAL        *NORMAL, *HIGH

 F3=Exit   F5=Refresh   F12=Cancel
```

Figure 4-10 Setting system value QTHDRSCAFN

4.3 Memory tuning

Note: A *memory-constrained system* is referred to several times in this chapter. In the context of performance tuning recommendations for WebSphere Portal Express, a memory-constrained system is a system with less than 5 GB of total memory or less than 4.5 GB of memory dedicated to a WebSphere Portal Express instance.

This section describes how to tune the memory resources of the system to enhance WebSphere Portal Express performance.

By default, WebSphere servers (Application Server or WebSphere Portal) are configured to run in the *BASE memory pool. If the system (or the logical partition for multiple LPARs system) where WebSphere Portal Express is running is not dedicated, then we recommend that you configure WebSphere Portal Express to run in its own memory pool. This helps better manage the memory resource utilization.

Note: If you decide to keep the default settings to run WebSphere Portal Express in the *BASE memory pool, then skip the following section, 4.3.1, “Running WebSphere Portal in a dedicated memory pool” on page 121 and apply the memory tuning guidelines to the *BASE memory pool.

4.3.1 Running WebSphere Portal in a dedicated memory pool

To run WebSphere Portal in a dedicated memory pool, perform the following steps:

1. Use the i5/OS CL command of Work with Shared Pools (WRKSHRPOOL) to manage the shared memory pools of your system (Figure 4-11 on page 121).

```
                        Work with Shared Pools
                                                              System:   RCHAS60
Main storage size (M)  . :       29695.99

Type changes (if allowed), press Enter.

              Defined    Max   Allocated   Pool  -Paging Option--
Pool         Size (M)  Active  Size (M)     ID   Defined  Current
*MACHINE      1394.55   +++++     1394.55    1   *FIXED   *FIXED
*BASE        25107.59    3590    25107.59    2   *FIXED   *FIXED
*INTERACT     3193.59    1299     3193.59    3   *FIXED   *FIXED
*SPOOL            .25       5         .25    4   *FIXED   *FIXED
*SHRPOOL1         .00       0                  *FIXED
*SHRPOOL2         .00       0                  *FIXED
*SHRPOOL3         .00       0                  *FIXED
*SHRPOOL4         .00       0                  *FIXED
*SHRPOOL5         .00       0                  *FIXED
*SHRPOOL6         .00       0                  *FIXED
                                                                      More...
Command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display tuning data
F12=Cancel
```

Figure 4-11 Work with Shared Pools

2. Select the first available shared memory pool (*SHRPOOL1 in this example) and set the memory pool size and activity level as shown in Figure 4-12. See 4.3.2, “Memory pool size” on page 122 and 4.3.3, “Memory pool activity level” on page 123 for the recommended values.

```
                        Work with Shared Pools
                                                              System:   RCHAS60
Main storage size (M)  . :       29695.99

Type changes (if allowed), press Enter.

              Defined    Max   Allocated   Pool  -Paging Option--
Pool         Size (M)  Active  Size (M)     ID   Defined  Current
*MACHINE      1394.55   +++++     1394.55    1   *FIXED   *FIXED
*BASE        25107.59    3590    25107.59    2   *FIXED   *FIXED
*INTERACT     3193.59    1299     3193.59    3   *FIXED   *FIXED
*SPOOL            .25       5         .25    4   *FIXED   *FIXED
*SHRPOOL1     5120.00     600                    *FIXED
*SHRPOOL2         .00       0                    *FIXED
*SHRPOOL3         .00       0                    *FIXED
*SHRPOOL4         .00       0                    *FIXED
*SHRPOOL5         .00       0                    *FIXED
*SHRPOOL6         .00       0                    *FIXED
                                                                    More...
Command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display tuning data
F12=Cancel
```

Figure 4-12 Configuring a shared memory pool

3. Configure the subsystem where WebSphere Portal Express V6 is running (QWAS6/QWAS6) to use that shared memory pool:
   a. Change the subsystem description:

      ```
      CHGSBSD SBSD(QWAS6/QWAS6) POOLS((2 *SHRPOOL1))
      ```

   b. Change the routing entry for that subsystem:

      ```
      CHGRTGE SBSD(QWAS6/QWAS6) SEQNBR(9999) POOLID(2)
      ```

4.3.2 Memory pool size

The *memory pool size* value is the amount of memory available for that memory pool. The minimum recommended value is 4 GB for the memory pool where WebSphere Portal is running (Figure 4-13 on page 123). Make sure that the faulting page rate remains under 100 pages per second.

Note 1: Allow more memory to the memory pool if other processes than WebSphere Portal Express are running in this memory pool.

Note 2: While tuning this parameter, monitor the disk utilization and ensure that it remains less than 25%. Also, monitor the faulting rate for the memory pool and ensure that it is under 100 pages per second.

```
                        Work with Shared Pools
                                                                System:   RCHAS60
Main storage size (M)  . :       29695.99

Type changes (if allowed), press Enter.

              Defined    Max   Allocated   Pool  -Paging Option--
Pool         Size (M)  Active  Size (M)     ID   Defined  Current
*MACHINE      1394.55   +++++     1394.55    1   *FIXED   *FIXED
*BASE        25107.59    3590    25107.59    2   *FIXED   *FIXED
*INTERACT     3193.59    1299     3193.59    3   *FIXED   *FIXED
*SPOOL            .25       5         .25    4   *FIXED   *FIXED
*SHRPOOL1     4096.00     600                    *FIXED
*SHRPOOL2         .00       0                    *FIXED
*SHRPOOL3         .00       0                    *FIXED
*SHRPOOL4         .00       0                    *FIXED
*SHRPOOL5         .00       0                    *FIXED
*SHRPOOL6         .00       0                    *FIXED
                                                                       More...
Command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display tuning data
F12=Cancel
```

Figure 4-13 Setting the memory pool size

4.3.3 Memory pool activity level

The memory pool activity level parameter controls the maximum number of eligible threads that can compete at the same time for storage in the memory pool. If the activity level is too low, the threads might transition to an ineligible condition. If the activity level is too high, excessive page faulting might occur.

To set this value, use the i5/OS CL command of Work with Active Jobs (WRKACTJOB) and press PF11 twice to display thread data for all jobs running in the memory pool. Calculate the sum of all the jobs in this memory pool and add 15%. Set the resulting value as the activity level for that memory pool using the i5/OS CL command of Work with Shared Pools (WRKSHRPOOL) as shown in Figure 4-14 on page 124. The minimum recommended value is 600.

Note: Regularly monitor the activity level of this memory pool and increase its value if the rate of transition from wait-to-ineligible is approaching the rate of active-to-wait.

```
                        Work with Shared Pools
                                                              System:   RCHAS60
Main storage size (M)  . :       29695.99

Type changes (if allowed), press Enter.

              Defined    Max   Allocated   Pool  -Paging Option--
Pool         Size (M)  Active  Size (M)     ID   Defined  Current
*MACHINE      1394.55   +++++     1394.55    1   *FIXED   *FIXED
*BASE        25107.59    3590    25107.59    2   *FIXED   *FIXED
*INTERACT     3193.59    1299     3193.59    3   *FIXED   *FIXED
*SPOOL            .25       5         .25    4   *FIXED   *FIXED
*SHRPOOL1     5120.00     600                    *FIXED
*SHRPOOL2         .00       0                    *FIXED
*SHRPOOL3         .00       0                    *FIXED
*SHRPOOL4         .00       0                    *FIXED
*SHRPOOL5         .00       0                    *FIXED
*SHRPOOL6         .00       0                    *FIXED
                                                                    More...
Command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display tuning data
F12=Cancel
```

Figure 4-14 Setting the memory pool activity level

4.3.4 Memory pool expert cache

The *memory pool expert cache* is an operating system function. Enabling this function can improve performance of applications that access data sequentially.

To enable this function, use the i5/OS CL command of Work with Shared Pools (WRKSHRPOOL). Then press PF11 for paging data and replace *FIXED with *CALC for the selected memory pool. See Figure 4-15 on page 125.

```
                        Work with Shared Pools
                                                                System:   RCHAS60
Main storage size (M)  . :       29695.99

Type changes (if allowed), press Enter.

              Defined    Max   Allocated   Pool  -Paging Option--
Pool         Size (M)  Active  Size (M)     ID   Defined  Current
*MACHINE      1394.55   +++++     1394.55    1   *FIXED   *FIXED
*BASE        25107.59    3590    25107.59    2   *FIXED   *FIXED
*INTERACT     3193.59    1299     3193.59    3   *FIXED   *FIXED
*SPOOL            .25       5         .25    4   *FIXED   *FIXED
*SHRPOOL1     5120.00     600                    *CALC
*SHRPOOL2         .00       0                    *FIXED
*SHRPOOL3         .00       0                    *FIXED
*SHRPOOL4         .00       0                    *FIXED
*SHRPOOL5         .00       0                    *FIXED
*SHRPOOL6         .00       0                    *FIXED
                                                                       More...
Command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display tuning data
F12=Cancel
```

Figure 4-15 Enabling the memory pool expert cache

4.4 Disk tuning

To determine if disks are a bottleneck on your system, check the disk utilization rate of each disk unit. We highly recommend that no one disk arm exceeds the limit of 25%.

Monitor your system disk utilization by using the i5/OS CL command of Work with Disk Status (WRKDSKSTS) and check the % Busy column. See Figure 4-16 on page 126.

```
                              Work with Disk Status                    RCHAS60
                                                                 04/11/07  09:31:49
Elapsed time:   00:00:06

               Size    %     I/O   Request   Read  Write   Read  Write    %
Unit  Type      (M)  Used    Rqs  Size (K)    Rqs   Rqs     (K)   (K)   Busy
   1  4326    30769  34.7     .0       .0     .0    .0      .0    .0      0
   2  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
   3  4326    30769  28.1     .1      4.0     .1    .0    4.0     .0      0
   4  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
   5  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
   6  4326    30769  28.1     .8      4.0     .8    .0    4.0     .0      0
   7  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
   8  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
   9  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
  10  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
  11  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
  12  4326    30769  28.1     .0       .0     .0    .0      .0    .0      0
  13  4326    30769  28.1     .1      4.0     .1    .0    4.0     .0      0
                                                                    More...
Command
===>
F3=Exit   F5=Refresh   F12=Cancel   F24=More keys
```

Figure 4-16 Work with Disk Status

4.5 Machine setup

This section provides information about how to set up the system to enhance WebSphere Portal Express performance.

4.5.1 Processors

If you are going to run WebSphere Portal Express on a mono-partition system, you need at least one processor with L3 cache.

For a system with multiple LPARs, the partition in which WebSphere Portal is going to run needs an integer number of processing units (avoid partial processing units at all costs). This avoids L1/L2 CPU cache flushes and any memory-intense application can benefit. WebSphere Application Server performance is dependent on the efficiency of L1/L2 CPU caches. If possible, allocate an even number of processing units to the WebSphere Portal partition.

4.5.2 Direct Access Storage Devices

The number of Direct Access Storage Devices (DASD) arms of the system yields the recommended disk utilization rate (see 4.4, “Disk tuning” on page 125). The minimum recommended value is 6 arms. A higher value helps to keep the disk utilization rate at an acceptable level.

You can monitor the disk status using the i5/OS CL command of Work with Disk Status (WRKDSKSTS). On the Work with Disk Status display, press PF11 and make sure that all

disks are in an ACTIVE status as shown in Figure 4-17. Take corrective action if the status shows any other value (for example, DEGRADED or FAILED).

```
                          Work with Disk Status                      RCHAS60
                                                                04/11/07  09:31:49
Elapsed time:   00:00:06

           --Protection--
Unit  ASP  Type  Status    Compression
   1    1  DPY   ACTIVE
   2    1  DPY   ACTIVE
   3    1  DPY   ACTIVE
   4    1  DPY   ACTIVE
   5    1  DPY   ACTIVE
   6    1  DPY   ACTIVE
   7    1  DPY   ACTIVE
   8    1  DPY   ACTIVE
   9    1  DPY   ACTIVE
  10    1  DPY   ACTIVE
  11    1  DPY   ACTIVE
  12    1  DPY   ACTIVE
  13    1  DPY   ACTIVE
                                                                      More...
Command
===>
F3=Exit   F5=Refresh   F12=Cancel   F24=More keys
```

Figure 4-17 DASD status

4.5.3 PTFs

Make sure that the Group PTFs are at the current levels. Table 4-8 lists the required group PTFs for i5/OS V5R3 and V5R4.

Table 4-8 Group PTFs for i5/OS V5R3 and V5R4

V5R3	V5R4
SF99530 Cumulative V5R3 SF99301 WebSphere Application Server V6.0 SF99503 DB2 UDB for iSeries SF99269 Java SF99099 IBM HTTP Server for iSeries	SF99540 Cumulative V5R4 SF99312 WebSphere Application Server V6.0 SF99504 DB2 UDB for iSeries SF99291 Java SF99114 IBM HTTP Server for iSeries

Note: Applying the latest level of Group PTFs for WebSphere Application Server V6.0 also applies the latest Group PTFs for DB2, Java, and HTTP.

You can check the latest levels available for Group PTFs at the following Web sites:

- For V5R3:

  http://www-912.ibm.com/s_dir/slineO03.NSF/GroupPTFs?OpenView&Start=1&Count=30&Expand=2#2

- For V5R4:

  http://www-912.ibm.com/s_dir/slineO03.NSF/GroupPTFs?OpenView&Start=1&Count=30&Expand=1#1

4.6 TCP/IP

This section describes the tuning for TCP/IP to enhance WebSphere Portal Express performance.

4.6.1 Line speed and duplex support

The line speed and duplex parameters set the line speed (in bits per second) and the *duplex support* (whether your system can send and receive data simultaneously over the line).

For both parameters, the recommended value is *AUTO. This causes the hardware to determine which values are used while using auto-negotiation.

To set these parameters, you can use the following i5/OS CL command of Change Line Description (Ethernet):

```
CHGLINETH LIND(line_name) LINESPEED(*AUTO) DUPLEX(*AUTO)
```

4.6.2 Maximum frame size

The maximum frame size parameter specifies the maximum frame size in bytes that you can transmit and receive over the line.

The recommended value is:

- 1496 bytes if the line speed < 1 Gigabit per second
- 8996 bytes if the line speed = 1 Gigabit per second

To set this parameter, you can use the following i5/OS CL command of Change Line Description (Ethernet):

```
CHGLINETH LIND(line_name) MAXFRAME(value)
```

4.6.3 Maximum transmission unit

The *maximum transmission unit (MTU)* parameter specifies the maximum number of bytes allowed in any datagram transmitting over the line. The recommended value is *LIND for the interface (value set by the line description) and *IFC for the corresponding route (value set by the interface using this route).

TCP/IP interface

To check the actual value, use the i5/OS CL command of Configure TCP/IP (CFGTCP) and select option 1 (Work with TCP/IP interfaces). Then select your interface from the list and display the details using option 5 (Figure 4-18 on page 129).

```
                          Display TCP/IP Interface
                                                              System:   RCHAS60
Internet address . . . . . . . . . . . . . . . . :   9.5.92.25
Subnet mask  . . . . . . . . . . . . . . . . . . :   255.255.255.0
Line description . . . . . . . . . . . . . . . . :   ETHLINE
Alias name . . . . . . . . . . . . . . . . . . . :   *NONE
Alias name CCSID . . . . . . . . . . . . . . . . :   0
Line type  . . . . . . . . . . . . . . . . . . . :   *ELAN
Associated local interface . . . . . . . . . . . :   *NONE
Interface status . . . . . . . . . . . . . . . . :   Active
Type of service  . . . . . . . . . . . . . . . . :   *NORMAL
Maximum transmission unit  . . . . . . . . . . . :   *LIND
Automatic start  . . . . . . . . . . . . . . . . :   *YES

Press Enter to continue.

F3=Exit   F12=Cancel
```

Figure 4-18 Display TCP/IP interface, MTU setting

To change this parameter value, you can use the following i5/OS CL command of Change TCP/IP Interface (CHGTCPIFC):

```
CHGTCPIFC INTNETADR('interface_ip_address') MTU(*LIND)
```

TCP/IP route

To check the actual value, use the i5/OS CL command of Configure TCP/IP (CFGTCP) and select option 2 (Work with TCP/IP routes). Then, select the route from the list and display the details using option 5 (Figure 4-19).

```
                           Display TCP/IP Route
                                                              System:   RCHAS60
Route destination  . . . . . . . . . . . :   *DFTROUTE
Subnet mask  . . . . . . . . . . . . . . :   *NONE
Type of service  . . . . . . . . . . . . :   *NORMAL
Next hop . . . . . . . . . . . . . . . . :   9.5.92.1
Preferred binding interface  . . . . . . :   *NONE
Maximum transmission unit  . . . . . . . :   *IFC
Duplicate route priority . . . . . . . . :   5
Route metric . . . . . . . . . . . . . . :   1
Route redistribution . . . . . . . . . . :   *NO

Press Enter to continue.

F3=Exit   F12=Cancel
```

Figure 4-19 Display TCP/IP route, MTU setting

To change this parameter value, use the following i5/OS CL command of Change TCP/IP Route (CHGTCPRTE):

```
CHGTCPRTE RTEDEST('route_ip_address') SUBNETMASK('subnet_mask') MTU(*IFC)
```

4.6.4 Send and receive buffer sizes

The send and receive buffer size parameters specify what to allocate for the default receive buffer and send buffer sizes. The *receive buffer size* is the amount of data that the remote system can send before being read by the local application. The *send buffer size* provides a limit for the amount of data being sent over TCP. When the send buffer is full (limit has been reached), the local application cannot send more data until the number of outgoing bytes drops below the limit. This happens when the remote application acknowledges the data reception.

The recommended value is 65535 bytes (64K) for both parameters.

To set these values, you can use the following i5/OS CL command of Change TCP/IP Attributes (CHGTCPA):

```
CHGTCPA TCPRCVBUF(65535) TCPSNDBUF(65535)
```

Note: You *must* restart TCP/IP for this change to take effect.

4.7 HTTP Server

This section describes the tuning for the HTTP server to improve WebSphere Portal Express performance.

4.7.1 Traffic compression

Note: Use this parameter with extreme caution.

You configure your HTTP server to compress only outbound traffic, because the amount of data sent to a Web browser is usually much higher than the amount of data received from a Web browser. Unless your system is already CPU-bound (CPU utilization greater than 60%), the benefit of reducing the size of data sent by the server to the Web browser outweighs the CPU overhead that compression introduces.

Set this parameter on only if large amounts of data are to be sent by the server to the Web browser and if your system is not CPU-bound.

To set up the traffic compression parameter, perform the following steps:

1. Locate your HTTP server's configuration file. It is located in the following i5/OS integrated file system directory at:

   `/www/http_instance_name/config/httpd.conf`

2. Edit this file and append the directives shown in Table 4-9 on page 131 to the end of the file.

Table 4-9 Enabling GZIP compression

HTTP Directives for GZIP compression
LoadModule deflate_module /QSYS.LIB/QHTTPSVR.LIB/QZSRCORE.SRVPGM AddType application/zip .jar SetOutputFilter DEFLATE SetEnvIf “UserAgent” “^.” no-gzip SetEnvIf “UserAgent” “MSI[E].(5\.5|6\.0);” !no-gzip SetEnvIf “UserAgent” “^Mozilla/5.0” !no-gzip SetEnv gzip-only-text/html 1 SetEnvIfNoCase Request_URI “\.(js|css)$” gzip-only-text/html=0 # Uncomment out the following lines to log compression statistics to the deflate_log file #LogFormat “\”%r\” %{outstream}n/%{instream}n(%{ratio}n%%)” deflate # CustomLog logs/deflate_log deflate #LogMaint logs/deflate_log 7 0 #DeflateFilterNode Input instream #DeflateFilterNode Ouput outstream #DeflateFilterNode Ratio ratio

3. Stop and restart your HTTP server.

4.7.2 General server configuration

This section describes general server settings that you can adjust to improve WebSphere Portal Express performance.

Number of threads to process requests

This parameter specifies the maximum number of threads to process a request.

Set this parameter value to the maximum number of parallel clients that can connect simultaneously to the HTTP server. The minimum recommended value is 300. See the following General server configuration settings section for details about how to set up this parameter.

DNS host name lookups for logging, CGI, and SSI

This parameter enables DNS lookups so the host names can be logged and passed to CGIs/SSIs in the REMOTE_HOST environment variable. When enabled, for each Internet transaction, the server accesses the DNS server for information (IP address and name translation). These accesses cause significant overhead (CPU and I/O) and greatly reduce the system capacity.

We recommend that you disable this function to improve performance. See the following General server configuration settings section for details about how to set up this parameter.

General server configuration settings

Perform the following steps:

1. Open a Web browser and type the following URL:

   `http://your_system:2001/HTTPAdmin`

2. From the IBM Web Administration for i5/OS window, click the **Manage** tab, and then click the **HTTP Servers** tab. Select your HTTP server from the drop-down list as shown in Figure 4-20.

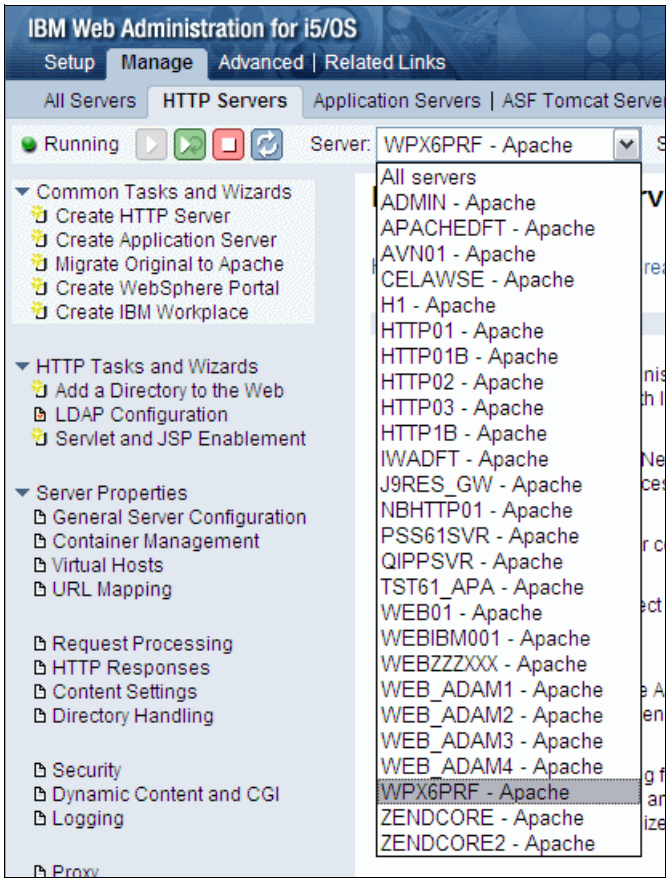


Figure 4-20 Selecting your HTTP server

3. Select **Server Properties** → **General Server Configuration**. On the General Server Configuration window, select the **General Settings** tab (Figure 4-21). On this window, you can set the number of threads to process requests and the DNS host name lookups for logging. Click **OK**.

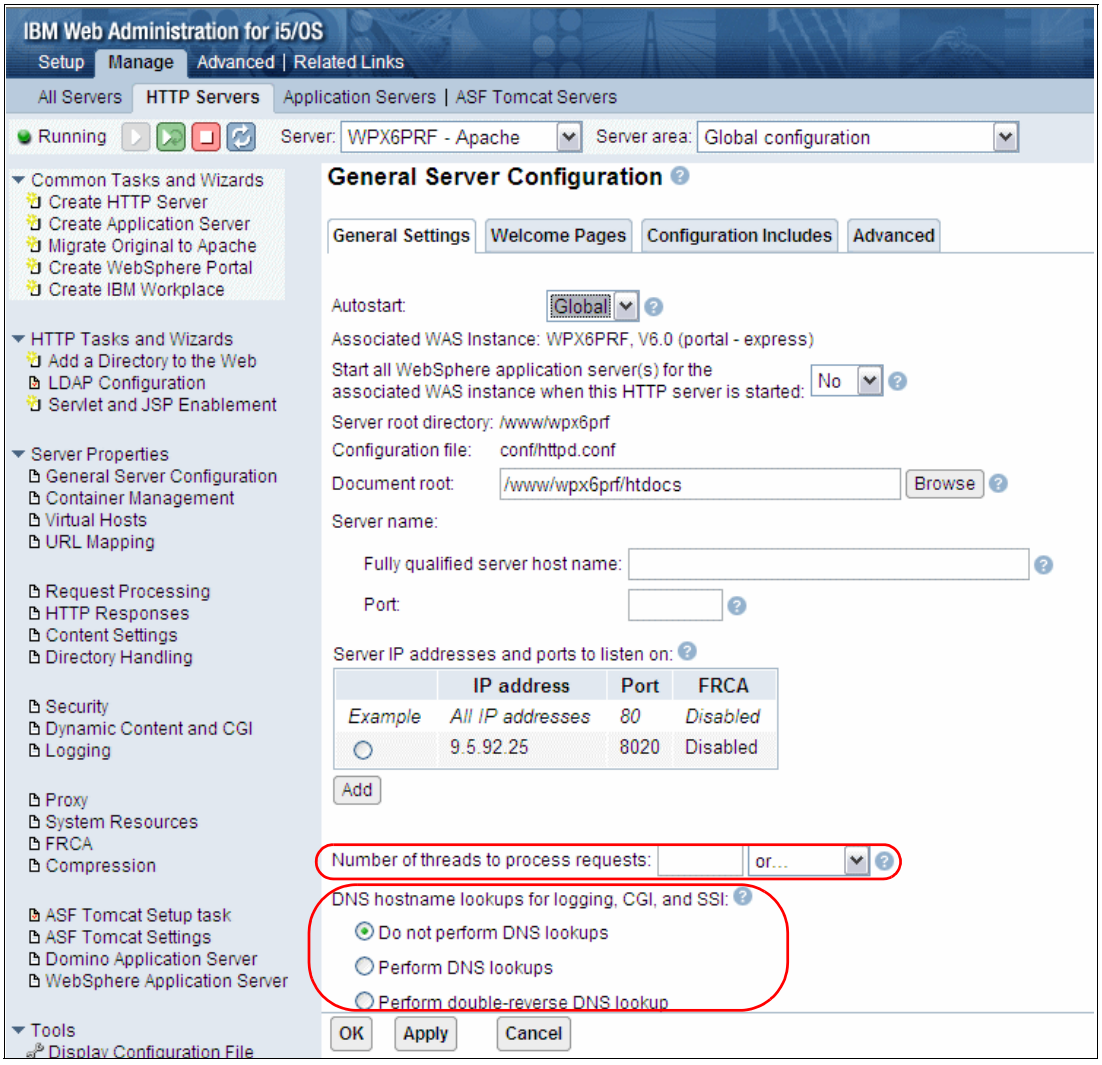


Figure 4-21 Setting up HTTP server general configuration

4.7.3 HTTP connections

This section describes how to control the client connections to your Web server by specifying the amount of time the server waits before timing out, the maximum length of the queue for pending connections, and the amount of time the server waits for a subsequent request before closing the connection.

Time to wait between requests: KeepAliveTimeout

This parameter sets the amount of time that the server waits for a subsequent request before closing the connection. The recommended value is above 5 minutes (300 seconds). See the following Setting up HTTP connection parameters section for details about how to set up this parameter.

Allow persistent connections: KeepAlive

This parameter enables a single TCP connection to be used for multiple HTTP requests (persistent connections). Normally, each HTTP request uses a separate connection. Reusing a single connection reduces the connection open/close overhead, thereby improving performance for that client. The recommended value is Enabled. See the following Setting up HTTP connection parameters section for details about setting up this parameter.

Maximum requests per connection: MaxKeepAliveRequests

This parameter limits the number of requests allowed on a persistent connection. The recommended value is unlimited. See the following Setting up HTTP connection parameters section for details about how to set up this parameter.

Setting up HTTP connection parameters

From the IBM Web Administration for i5/OS Web interface, select **Server Properties** → **System Resources**. On the System Resources page, select the **HTTP Connections** tab (Figure 4-22).

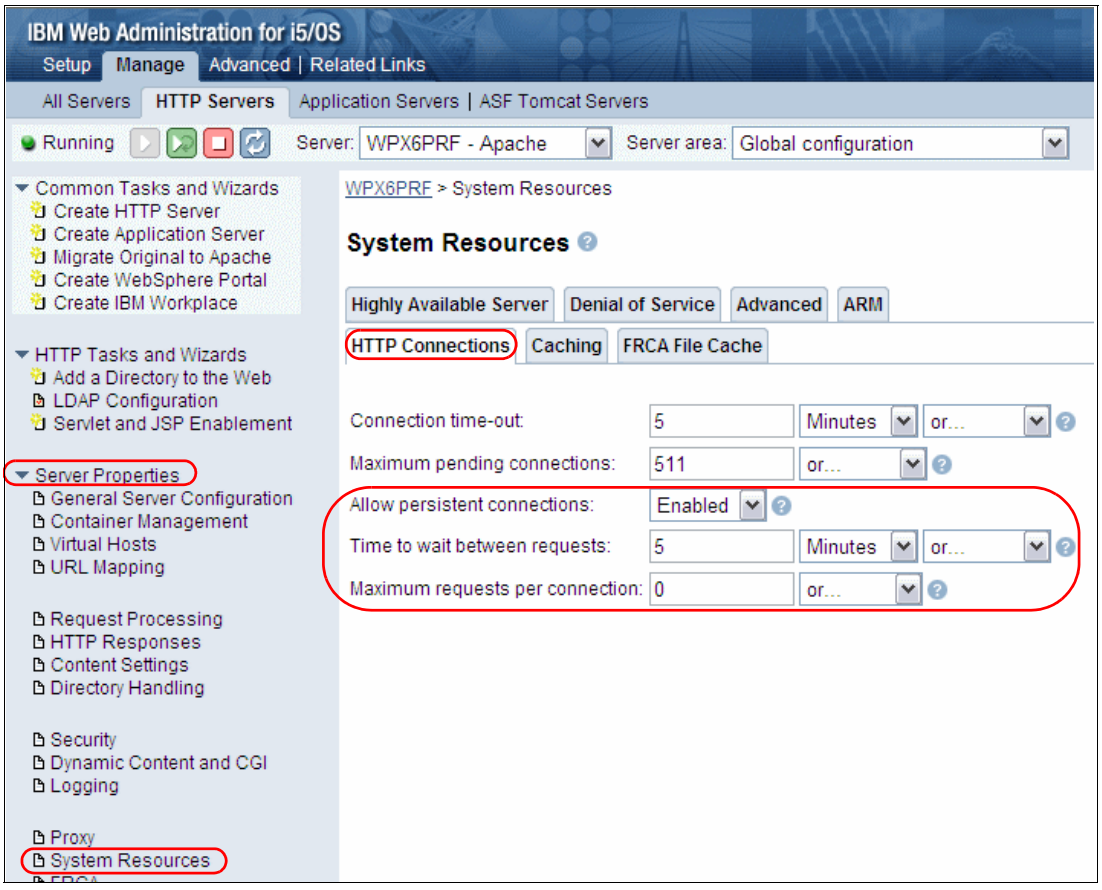


Figure 4-22 Setting up the HTTP connections parameters

4.7.4 Logging levels

By default, the IBM HTTP Server for iSeries provides two logs: an error log and an access log.

Error log

You can adjust the complexity of messages recorded in the error logs. When a particular level is specified, messages from all other levels of higher significance are reported. For example, when Critical is specified, then messages with log levels of Alert and Emergency are also posted.

You can find the error log file in the i5/OS integrated file system directory of /www/http_instance_name/logs/error_log.Q1*yymmdd*00, where *yymmdd* stands for year/month/date.

The recommended value for the error log level is Critical.

To set this parameter, from the IBM Web Administration for i5/OS Web interface, select **Server Properties** → **Logging**. On the Logging Web page, select the **Error Logs** tab (Figure 4-23). You must stop and restart the HTTP server for any changes to take effect.

Note: You can disable the error log, but we do *not* recommend doing so, because you might lose valuable information when you are troubleshooting.

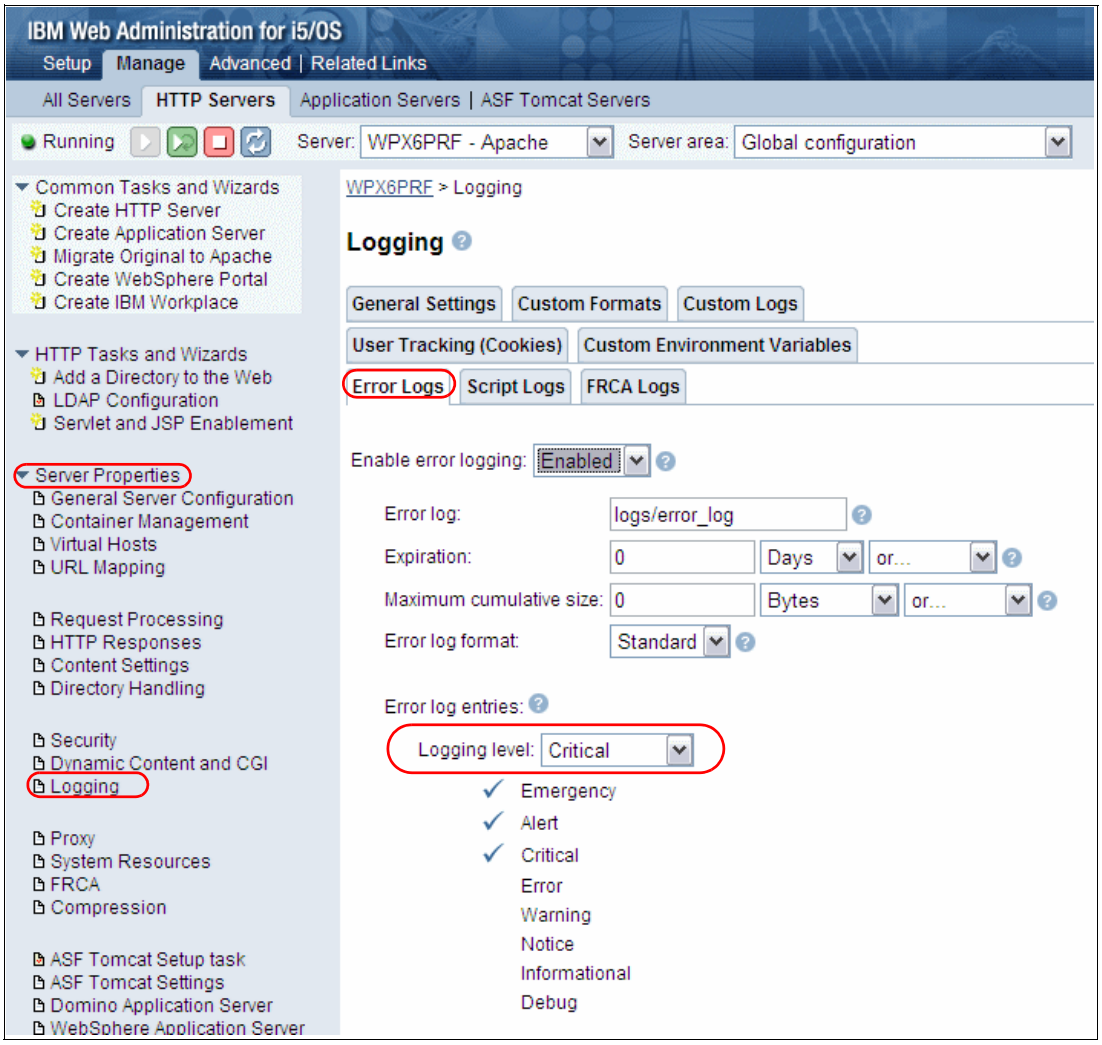


Figure 4-23 Setting up the HTTP server error log level

Access log

The HTTP server offers you the capability to define custom logs. The access log is one of them.

You can find the access log file in the i5/OS integrated file system directory of /www/http_instance_name/logs/access_log.Q1*yymmdd*00, where *yymmdd* stands for year/month/date.

We recommend that you disable this log for performance improvements.

From the IBM Web Administration for i5/OS interface, you can remove this log. See Figure 4-24.

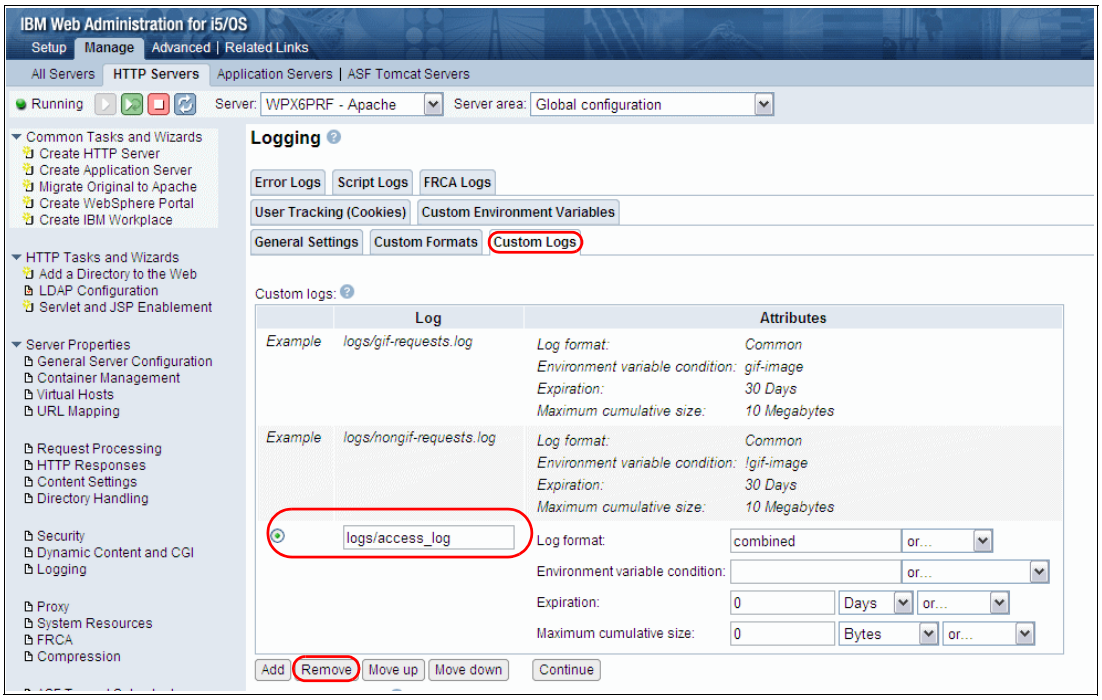


Figure 4-24 Removing HTTP server access log

Or, you can edit the HTTP server configuration file (see 4.7.1, “Traffic compression” on page 130 for information about the configuration file) and comment out the following directive:

```
#CustomLog logs/access_log combined
```

You *must* stop and restart the HTTP server for any changes to take effect.

Note: We recommend that you use the second option, because doing so makes it easier to re-enable it for troubleshooting purposes.

4.8 WebSphere Application Server

This section describes tuning WebSphere Application Server to improve portal performance.

4.8.1 Default application server

During the deployment of the WebSphere Portal Express instance, a default application server (*server1*) is created. It is used only during the deployment of the instance. When the deployment is complete, you can stop this server. Perform the following steps:

1. From the IBM Web Administration for i5/OS Web interface, select the **Manage** tab, then select the **All Servers** tab, and finally select the **All Application Servers** tab (Figure 4-25).

Figure 4-25 Managing applications servers

2. From the list of servers displayed, select the **server1** server that is associated with your portal from the list and click **Stop** (Figure 4-26).

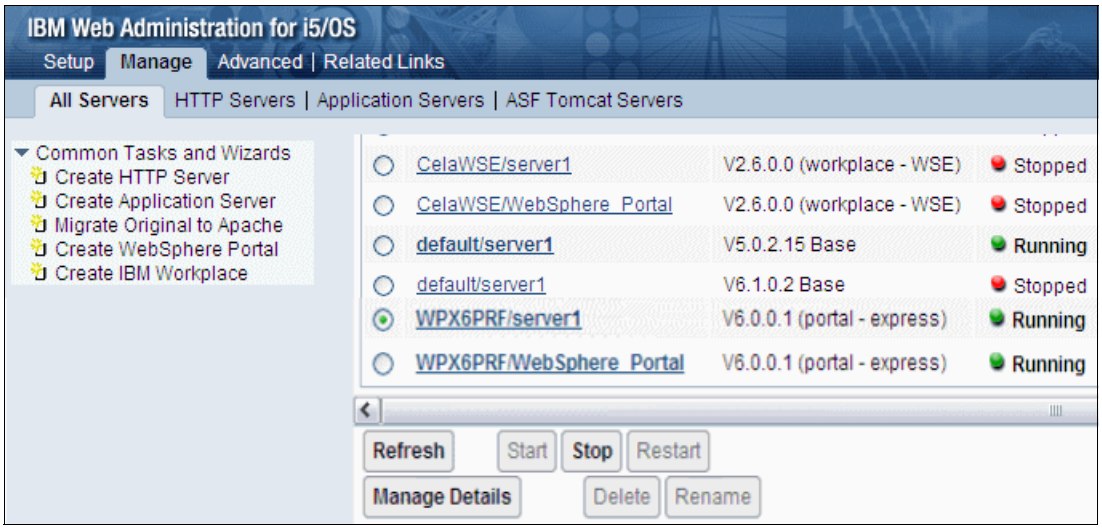


Figure 4-26 Stopping application server server1

4.8.2 Java Virtual Machine

The Java Virtual Machine (JVM) is one of the most critical areas in terms of performance. Improperly tuning the JVM results in poor performance and in some cases can cause WebSphere Portal Express to end abnormally.

Note: When a property of the JVM is modified using the WebSphere Application Server administrative console, the WebSphere Portal server needs to be stopped and restarted for that modification to become effective.

Heap size

You need to tune the JVM heap size so that the garbage collection runs at suitable intervals. Running too often causes unnecessary overhead, but you want to run it enough to prevent the heap from growing too large.

Increasing the size of the Java heap usually improves throughput until the heap no longer resides in physical memory. When the heap size exceeds the physical memory, the heap begins swapping to disk, which causes Java performance to drastically decrease. Therefore, it is important to set the maximum heap size to a value that allows the heap to be contained within physical memory.

To prevent paging, allow a minimum of 256 MB of physical memory for each processor and 512 MB of physical memory for each application server. If possible, adjust the available memory when paging occurs if processor utilization is low because of this paging.

Table 4-10 shows the recommended values for the initial Java heap size, depending on the physical memory.

Table 4-10 Initial heap size versus physical memory

Total system memory	Portal memory pool	Java heap size
Up to 6 GB	Up to 5 GB	256 MB
Up to 8 GB	Up to 7 GB	512 MB
More than 8 GB	More than 7 GB	768 MB

We recommend that you set the maximum heap size at a value that allows it to be contained within the physical memory. You can also set the maximum heap size to 0, which means no maximum for the heap, but ensure that you have enough physical memory to handle this setting.

For more information about JVM tuning, refer to the following Web page:

http://www.ibm.com/servers/enable/site/education/wp/c566/index.html

To change the Java heap size, perform the following steps:

1. From the IBM Web Administration for i5/OS Web interface, select your WebSphere portal instance and click **Tools** → **Launch Administrative Console** (Figure 4-27 on page 139).

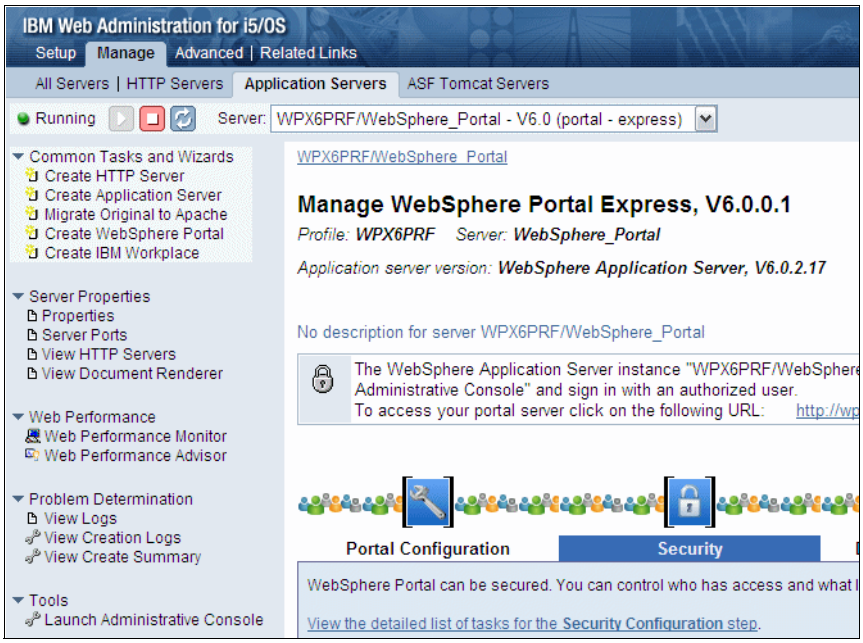


Figure 4-27 Launching the portal administrative console

2. Log in to the WebSphere Application Server administrative console, select **Servers** → **Application servers**, and click **WebSphere_Portal**. Under Server Infrastructure, select **Process Definition** (Figure 4-28).

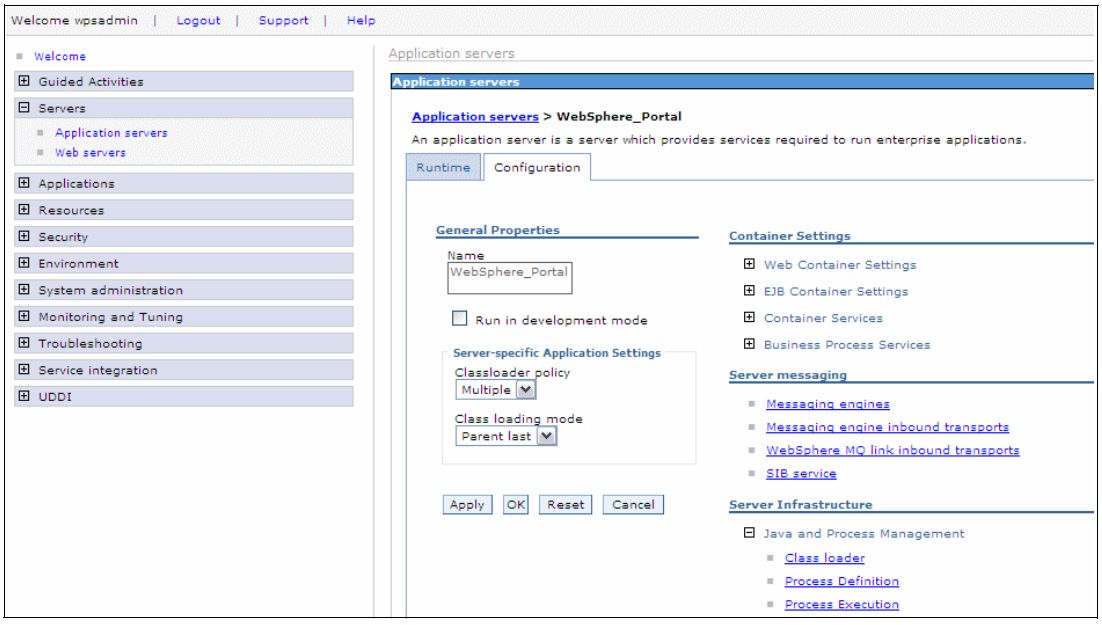


Figure 4-28 Managing the application server

3. On the Application servers page, under the Additional Properties section, select **Java Virtual Machine** (Figure 4-29).

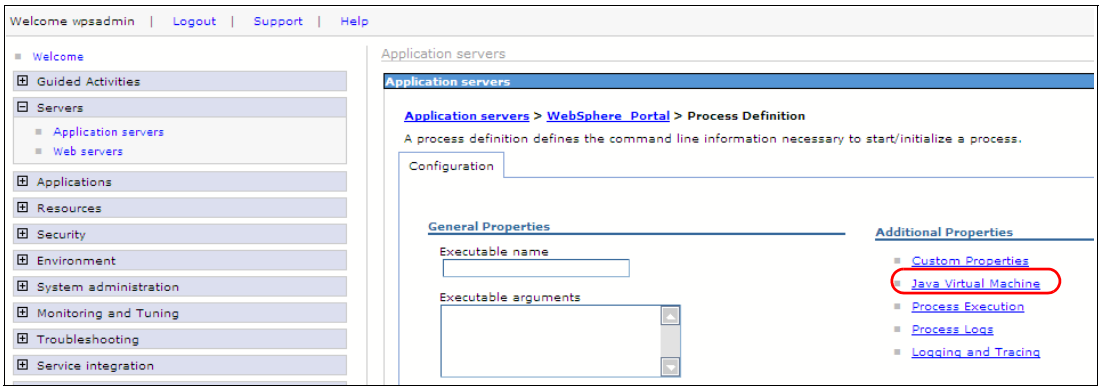


Figure 4-29 Managing the JVM

4. Set the desired heap size and click **OK** to accept the new values (Figure 4-30).

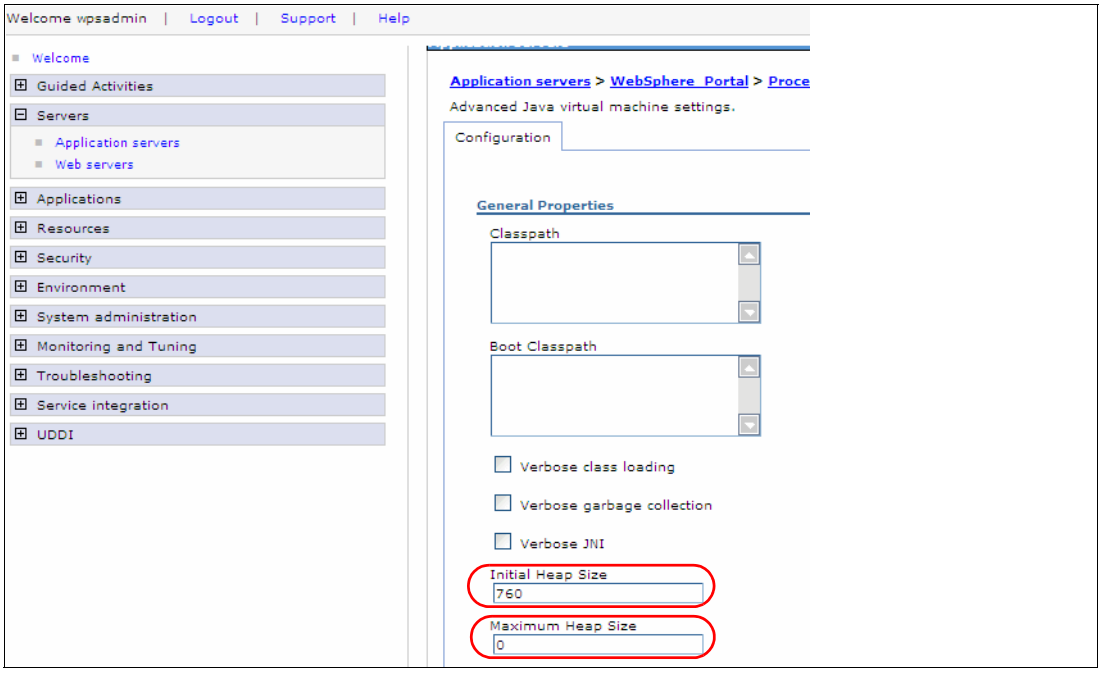


Figure 4-30 Setting up the JVM heap size

Garbage collection

You can set up the garbage collector for more class reuse, thus causing less garbage collection to occur.

Note: For memory-constrained systems, we recommend that you enable this parameter.

To change the garbage collector, perform the following steps:

1. Log in to the WebSphere Application Server administrative console. See “Heap size” on page 138 to launch the administrative console.
2. Select **Servers** → **Application servers**, click **WebSphere_Portal**, and under Server Infrastructure, select **Process Definition**. On the resulting page, select **Java Virtual**

Machine. In the **Generic JVM arguments** text field, add `-Xnoclassgc`, and click **OK** to confirm the change (Figure 4-31).

Note: The generic JVM arguments are case-sensitive. If you do not respect the case, the JVM does not restart after it is stopped.

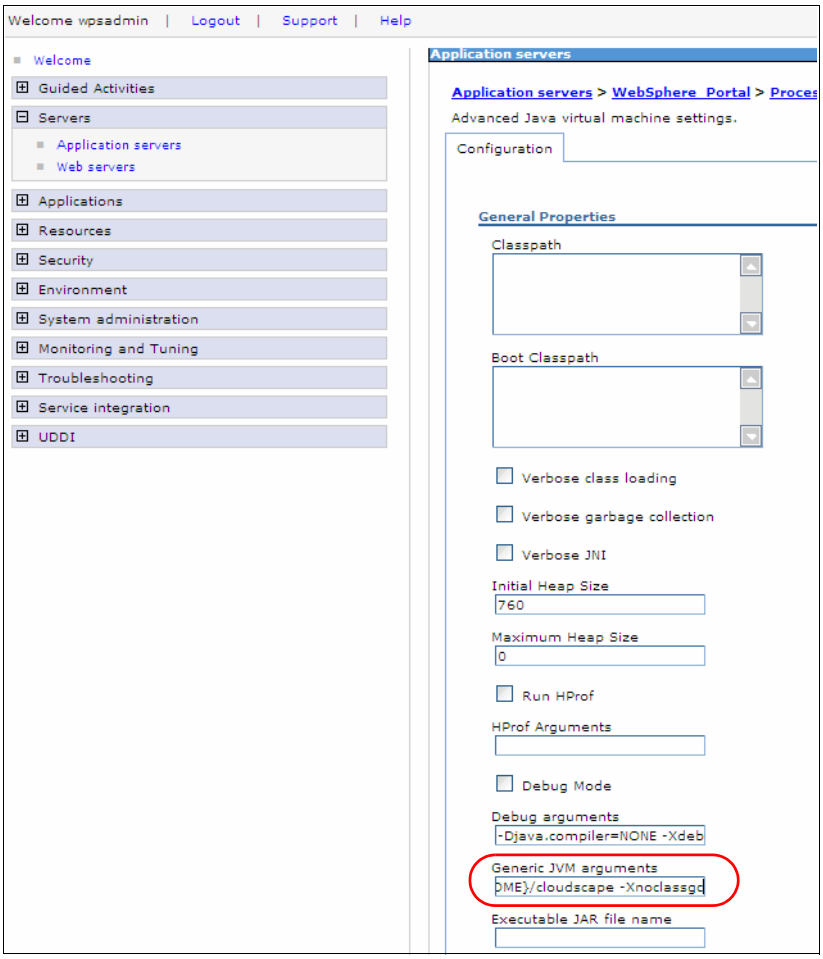


Figure 4-31 Tuning the JVM garbage collector

Java compiler

A *Just-In-Time (JIT) compiler* is a platform-specific compiler that generates machine instructions for each method as needed. Using the JIT compiler results in highly optimized code that improves runtime performance when compared to precompiled code. For more information about the JIT compiler, see the iSeries Information Center at:

`http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzaha/jit.htm`

By default, on the System i platform, the JIT compiler is enabled, but the JVM runs in a Mixed Mode Interpreter until the Java System value `os400.jit.mmi.threshold` is reached. Then, the JIT compiler compiles Java classes into machine instructions.

To enable full JIT compiling (not using Mixed Mode Interpreter), log in to the WebSphere Application Server administrative console of your portal server, select **Servers** → **Application servers**, click **WebSphere_Portal**, and under Server Infrastructure, select

Process Definition. On the resulting page, select **Java Virtual Machine**. In the **Generic JVM arguments** text field, add `-Djava.compiler=jitc`, and click **OK** to confirm the change (Figure 4-32).

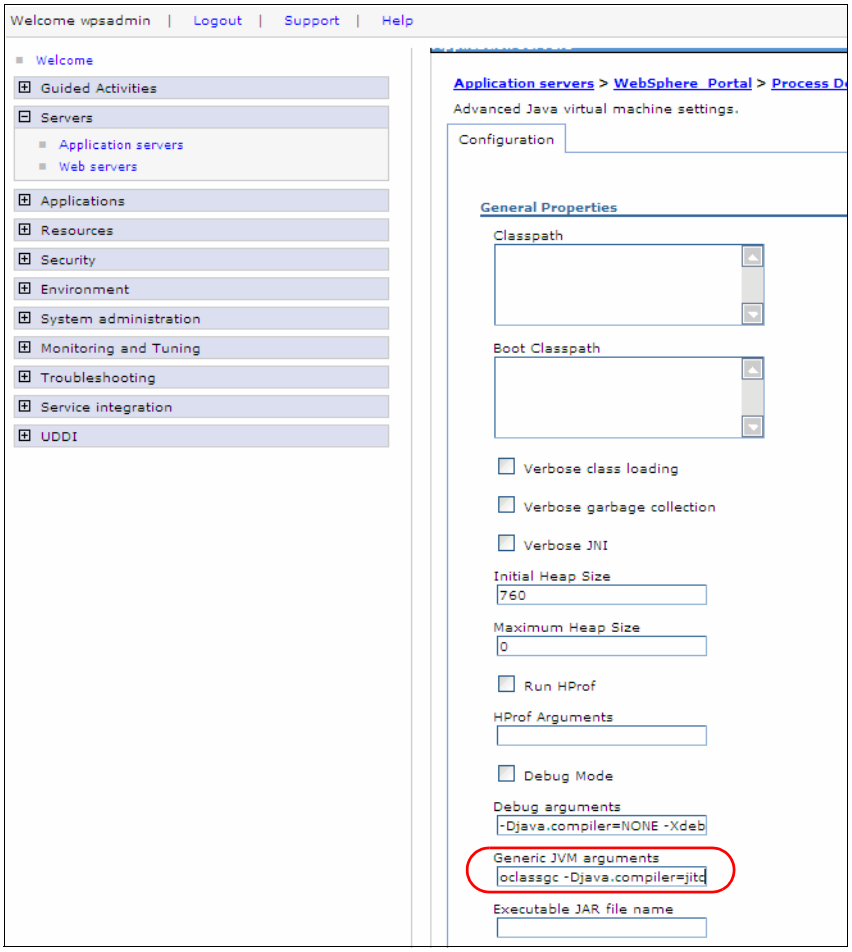


Figure 4-32 Enabling the full JIT compiler

4.8.3 Caching

Using caching improves performance because the resources being cached are directly available to be processed by the portal server.

User class loader cache

The JVM for i5/OS has a feature called *user class loader cache*. When you enable this feature, it allows the JVM to cache resources that are loaded using user class loader. That cache stores the optimized Java program objects, which enables the JVM to reuse them. Performance is improved, because the JVM does not need to recreate the optimized Java program objects, nor does it need to verify their bytecode. WebSphere components (servlets, JSPs, and enterprise beans) are loaded by user class loaders and can take advantage of this feature.

The optimized Java program objects are stored in the class loader cache jar file. This jar file is provided in the i5/OS integrated file system directory of /QIBM/ProdData/Java400/QDefineClassCache.jar. You can use it as is or copy it to another location and rename it.

You can also create your own cache jar file by performing the following steps:

1. Create your own user class loader cache jar file:
   a. Start Qshell using the i5/OS CL command of Start QSH (STRQSH).
   b. Switch to the directory where you want the JAR file located. Make the directory first, if necessary:

      ```
      mkdir /cache_path/cache
      cd /cache_path/cache
      ```

   c. Create a dummy file to place in the JAR. You can name it anything, the following example uses a file called example:

      ```
      touch example
      ```

   d. Create the user class loader cache jar file. The following example uses `MyCache.jar`:

      ```
      jar -cf MyCache.jar example
      ```

   e. Clean up the dummy file:

      ```
      rm example
      ```

2. Enable the user class loader cache:
   a. Log in to the WebSphere Application Server administrative console for the portal server and select **Servers** → **Applications Server**. Click **WebSphere_Portal** and under Server Infrastructure, select **Process Definition**. On the resulting page, select **Java Virtual Machine** and under Additional Properties, click **Custom Properties**.
   b. Click **New** to add a new property.
   c. Set the custom property name to `os400.define.class.cache.file`.
   d. Set the custom property value to the path of the user class loader cache jar file. In this example, it is `/cache_path/cache/MyCache.jar`.
   e. You can further tune the user class loader cache by defining the following custom properties:
      - *os400.define.class.cache.hours*: This property specifies how long an object persists in the cache in hours. The default value is 168 if this property is not specified.
      - *os400.define.class.cache.maxpgms*: This property specifies how many objects can persist in the cache. The default value is 5000 if this property is not specified.

      For example, if you want the cache to persist a maximum of 10000 objects for one year, then add the following custom property names and values:

      ```
      os400.define.class.cache.hours        8760
      os400.define.class.cache.maxpgms     10000
      ```

   f. Save the changes to the main configuration and restart the portal server.
3. To verify that the user class loader cache is active, use the i5/OS CL command of Display Java Program Information (DSPJVAPGM). For example:

   ```
   DSPJVAPGM CLSF('/cache_path/cache/MyCache.jar')
   ```

Edge Side Include cache

The Web server plug-in contains a built-in Edge Side Include (ESI) processor that caches whole pages and fragments, providing a higher cache hit ratio. The cache implemented by the ESI processor is an in-memory cache, not a disk cache; therefore, the cache entries are not persisted when the Web server is restarted.

To enable the ESI cache, stop the WebSphere Portal server and update the plug-in configuration file plugin-cfg.xml in the i5/OS integrated file system directory of /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/portal_instance/cells/cell_name/nodes/IHS_nodename_node/servers/IHS_servername/.

Update the following property:

```
<Property Name="ESIEnable" Value="true"/>.
```

Restart the WebSphere Portal server.

Important: If Secure Sockets Layer (SSL) is enabled, then you cannot enable ESI.

4.8.4 Servlet engine thread pool

A *thread pool* enables components of the server to reuse threads and eliminates the need to create new threads at run time. Creating new threads is a time and resource intensive operation.

To start, set the minimum and maximum thread pool size to 70/70. Then monitor the activity of that thread pool using the performance viewer that is built into the WebSphere Application Server administrative console. Increase this value if all servlet threads are busy most of the time. Decrease this value if all servlet threads are idle most of the time.

To change the servlet engine thread pool, perform the following steps:

1. Log in to the WebSphere Application Server administrative console, select **Servers** → **Application Server**, click **WebSphere_Portal**, and under Additional Properties, select **Thread Pools** (Figure 4-33 on page 145).

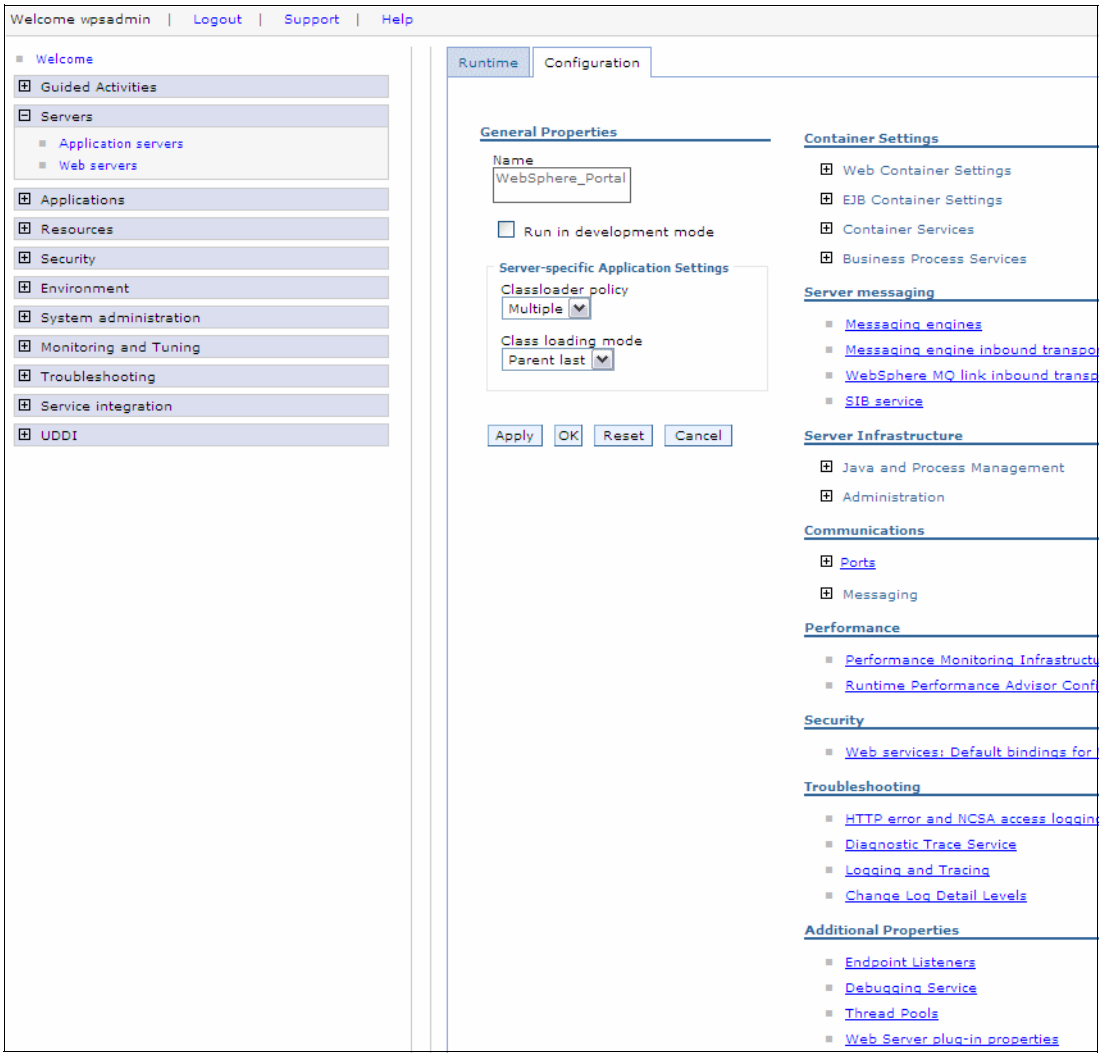


Figure 4-33 Managing thread pools

2. On the Thread Pools page, click **Web Container** (Figure 4-34).

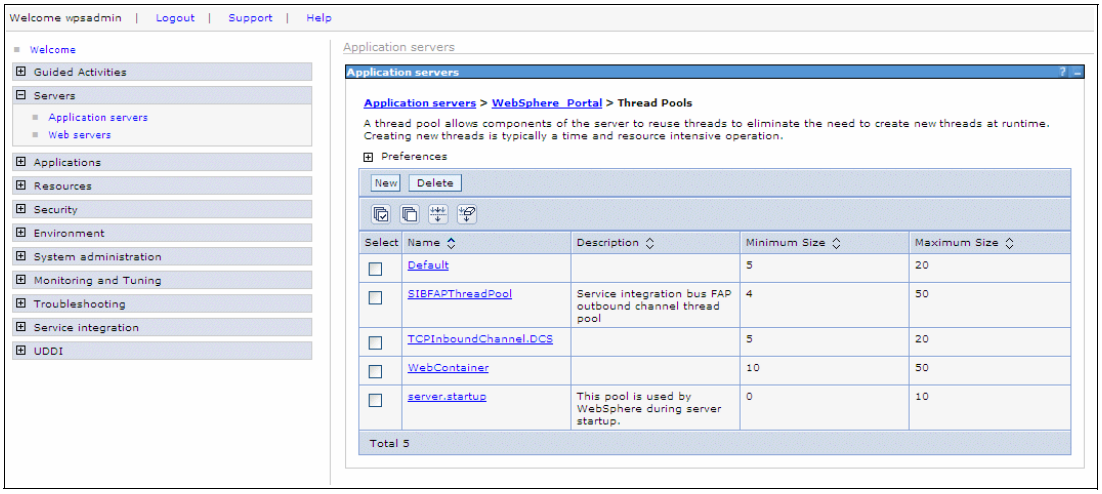


Figure 4-34 Web container thread pools

3. Set the desired values and click **OK** to accept the changes (Figure 4-35).

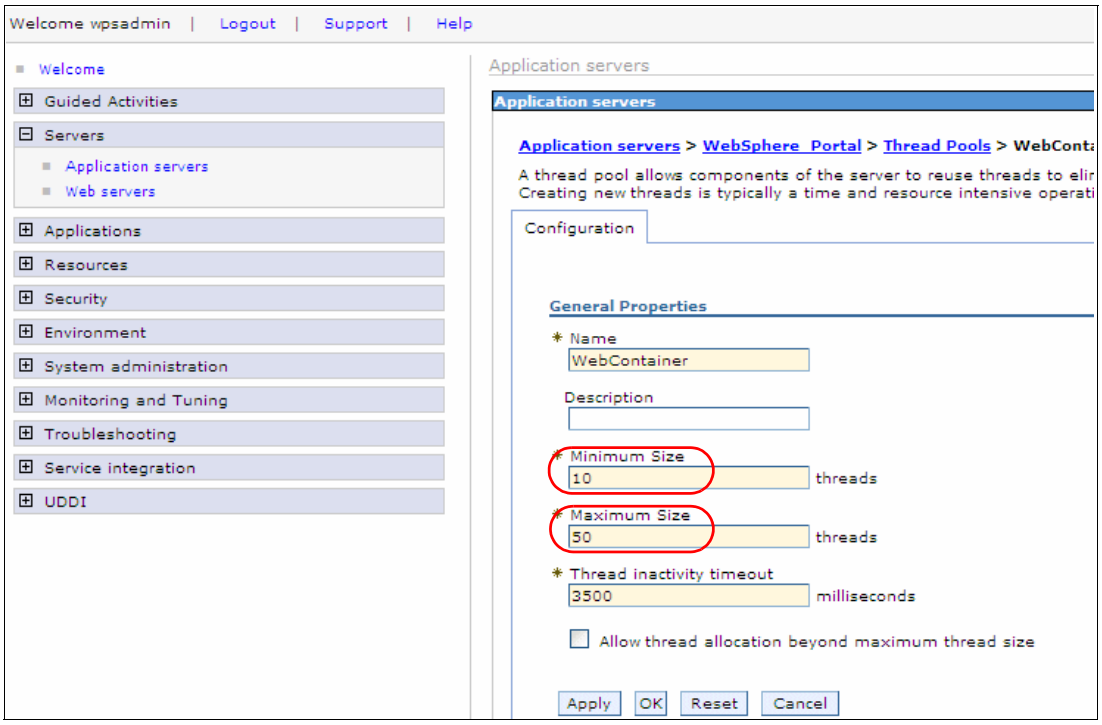


Figure 4-35 Setting up the servlet engine thread pool size

4. To monitor the thread pool activity, select **Monitoring and Tuning** → **Performance Viewer** → **Current Activity**, then click **WebSphere_Portal** (Figure 4-36).

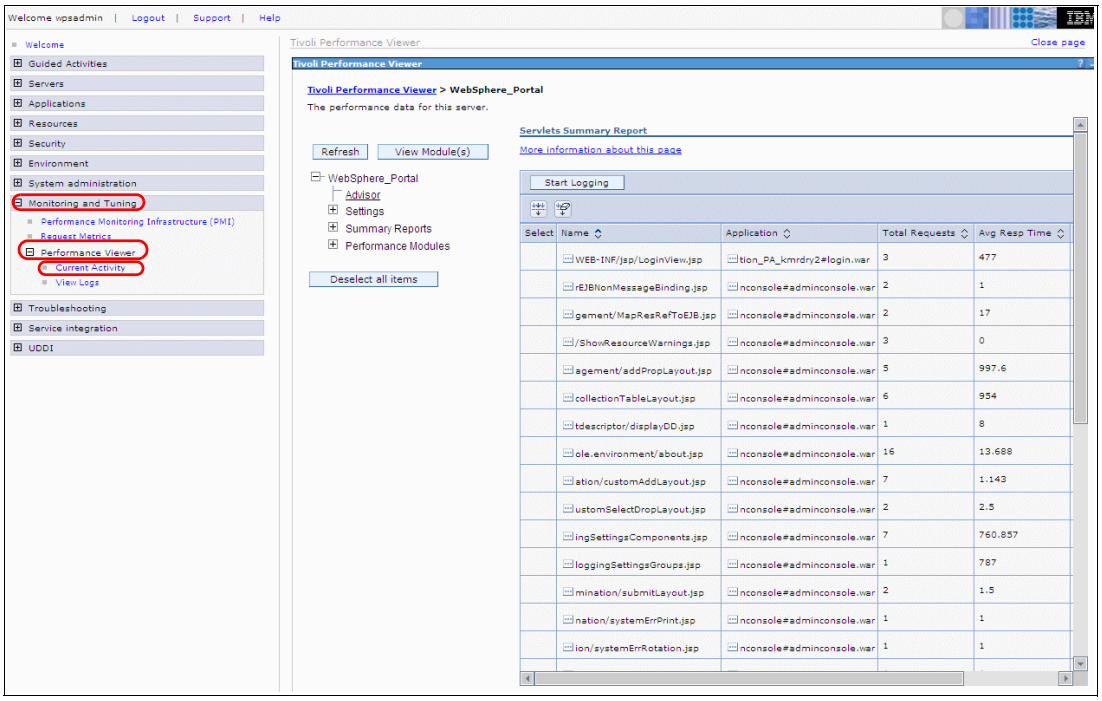


Figure 4-36 Monitoring tool

5. Expand **WebSphere_Portal** → **Performance Modules** → **Thread Pools** and check the **WebContainer** check box (Figure 4-37).

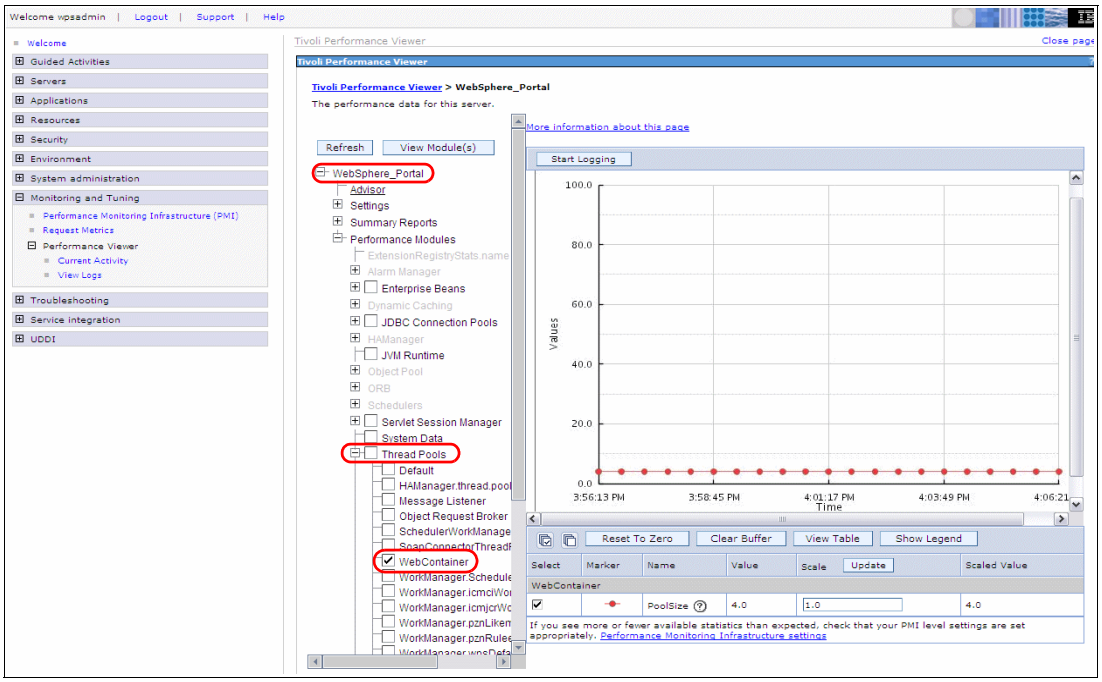


Figure 4-37 Monitoring thread pool activity

4.8.5 Session timeout

This parameter specifies how long a session can go unused before it is no longer valid. The value specified in a Web module deployment descriptor file takes precedence over the WebSphere Application Server administrative console settings. However, the value of this setting is used as a default when the session timeout is not specified in a Web module deployment descriptor. By default, the Web module deployment descriptor for WebSphere Portal Express does not specify this parameter.

The default value is set to 30 minutes. Set this parameter to a value that is acceptable by your users. Reducing this value too much interferes with the user experience by forcing the user to be logged out more frequently. Increasing this value too much can result in excessive memory consumption.

To change the session timeout value, perform the following steps:

1. Log in to the WebSphere Application Server administrative console, select **Servers** → **Application Servers**, click **WebSphere_Portal**. Under Container Settings, select **Web Container Settings** → **Session management** (Figure 4-38 on page 148).

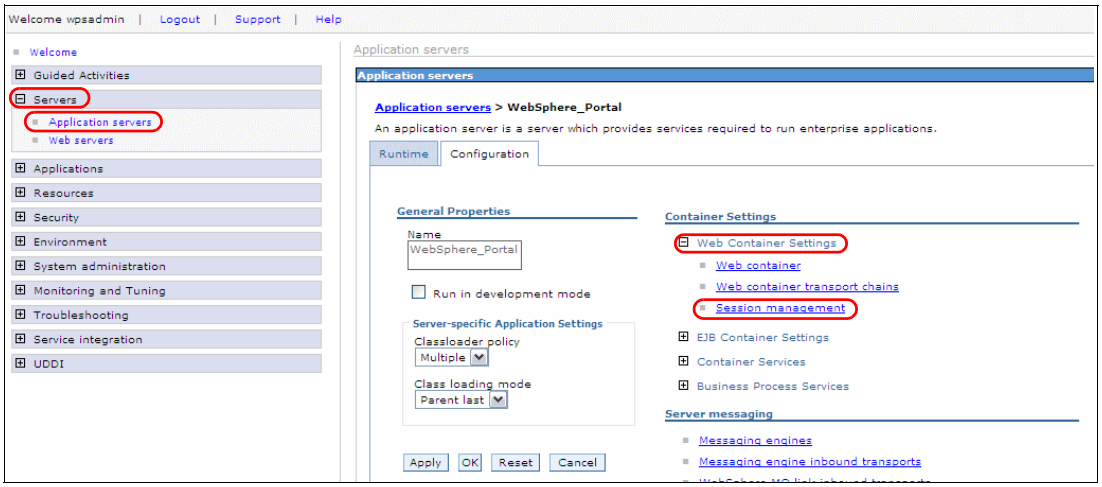


Figure 4-38 Managing the session timeout

2. Set the session timeout and click **OK** to accept the new value (Figure 4-39).

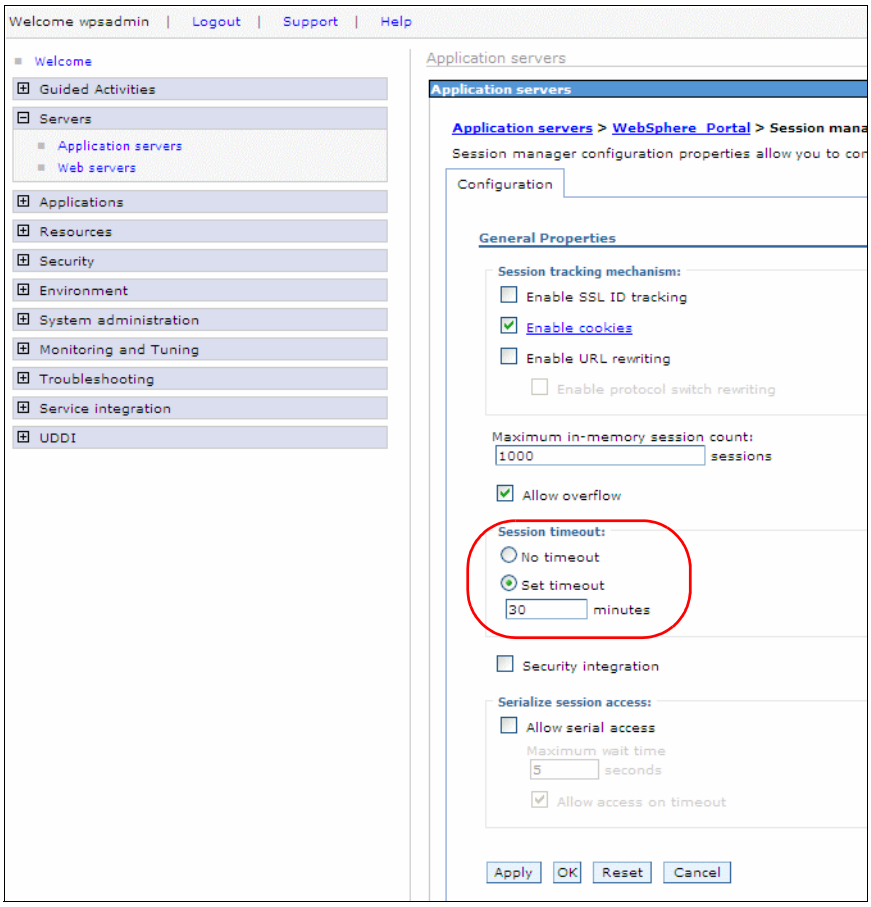


Figure 4-39 Setting up the session timeout

4.8.6 Logging level

By tuning log levels, you can control which events are processed by Java logging. When you change the level for a logger, the change is propagated to the children of the logger.

By default, WebSphere Portal Express is configured to log all events at an information level. We recommend that you set up this parameter at a logging level of severe. This causes less overhead in terms of CPU and I/O operations, but still enables the administrator to access valuable information for troubleshooting.

To change the logging level, perform the following steps:

1. Log in to the WebSphere Application Server administrative console, select **Servers** → **Application Servers**, click **WebSphere_Portal**, and under Troubleshooting, select **Change Log Detail Levels** (Figure 4-40).

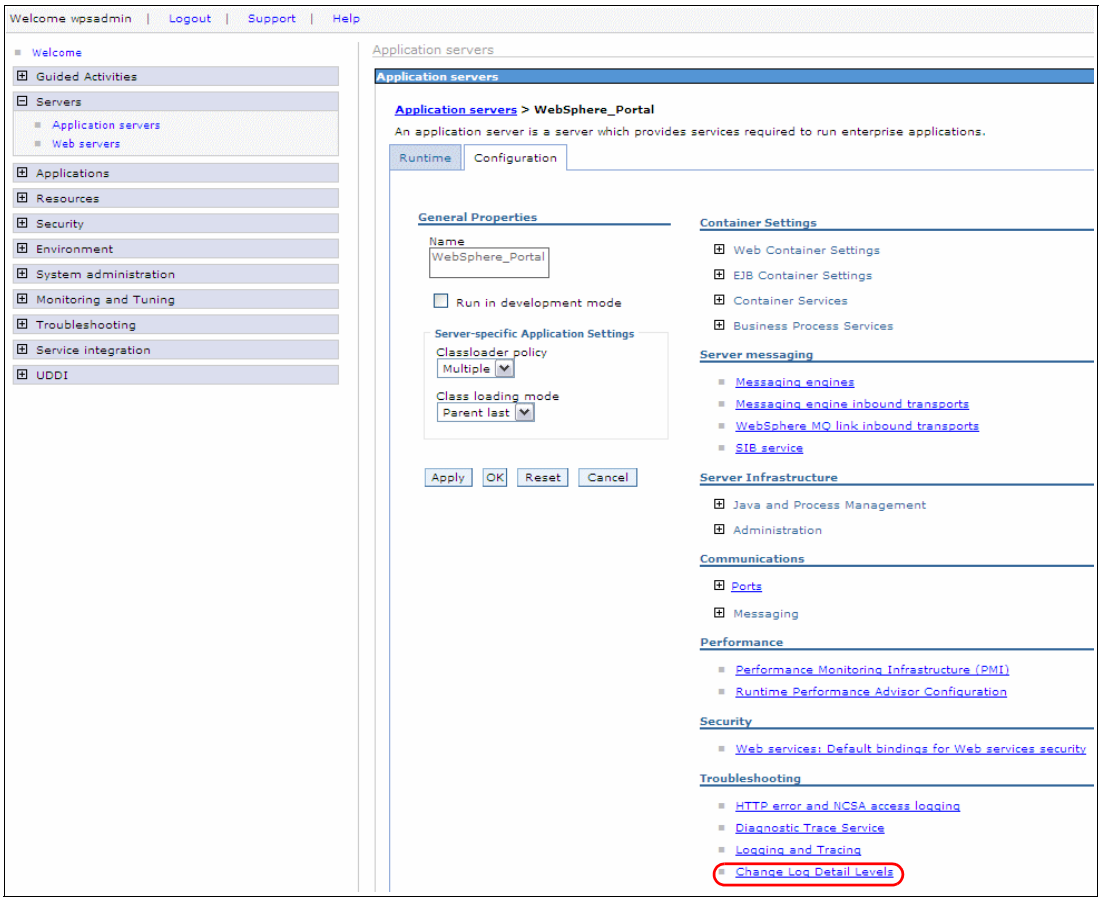


Figure 4-40 Application server logging

2. Set the parameter value to *=severe, and click **OK** to accept the new value (Figure 4-41).

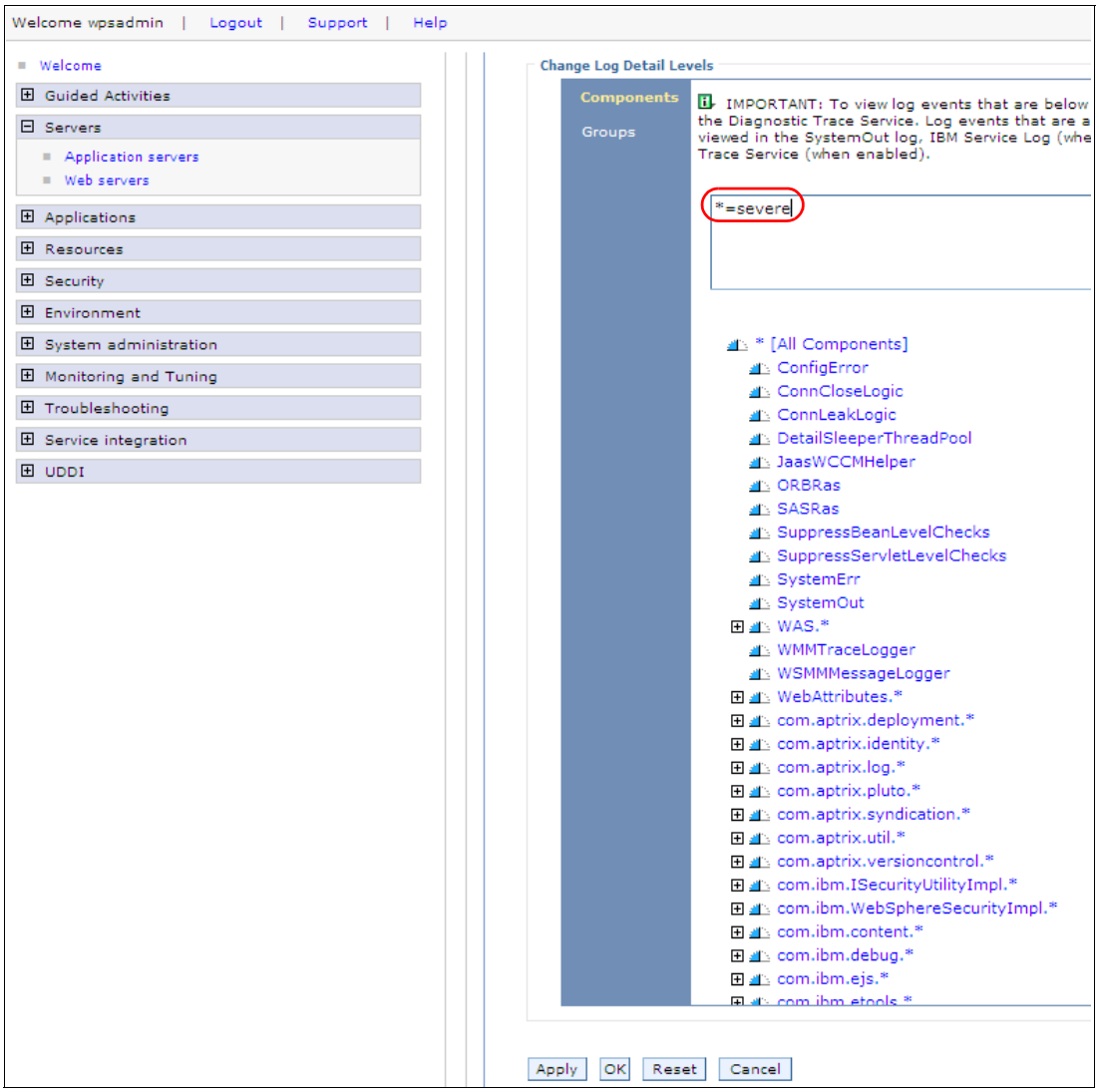


Figure 4-41 Setting up logging level

4.9 Database

This section describes how you can enhance the database performance. This section is only relevant to DB2 UDB for i5/OS.

We recommend a dedicated shared pool for the database server jobs. There are two sets of database server jobs:

QSQSRVR These jobs perform Call Level Interface DB2 USB SQL functions used by IBM functions, such as Management Central, and by Java-based applications performing SQL. By default, the priority of these jobs on the system is 10.

QZDSASOINIT These jobs perform ODBC/JDBC SQL functions requested by client workstations. By default, the priority of these jobs on the system is 20.

The QSQSRVR jobs have their own shared pool, or are in the same shared pool as the QZDSASOINIT database server jobs. Keeping the database server jobs running in the same pool as the portal JVM results in a negative impact on overall performances. See 4.3.1, “Running WebSphere Portal in a dedicated memory pool” on page 121 to dedicate shared memory pools to database server jobs (select different memory pools for the portal and the database server jobs).

5

Enabling Secure Sockets Layer

This chapter describes the process for implementing a secure WebSphere Portal environment. This process secures transactions and traffic between the various components participating in your WebSphere Portal environment. Securing transactions and traffic is done by using the Secure Sockets Layer (SSL) protocol, which encrypts the data before it is sent over an unprotected network (for example, the Internet). For more information about SSL, see the i5/OS Information Center at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzain/rzainoverview.htm

© Copyright IBM Corp. 2007. All rights reserved.

As shown in Figure 5-1, you can secure only the overall login process (1 to 4), or you can secure the whole portal content and the login (1 to 7).

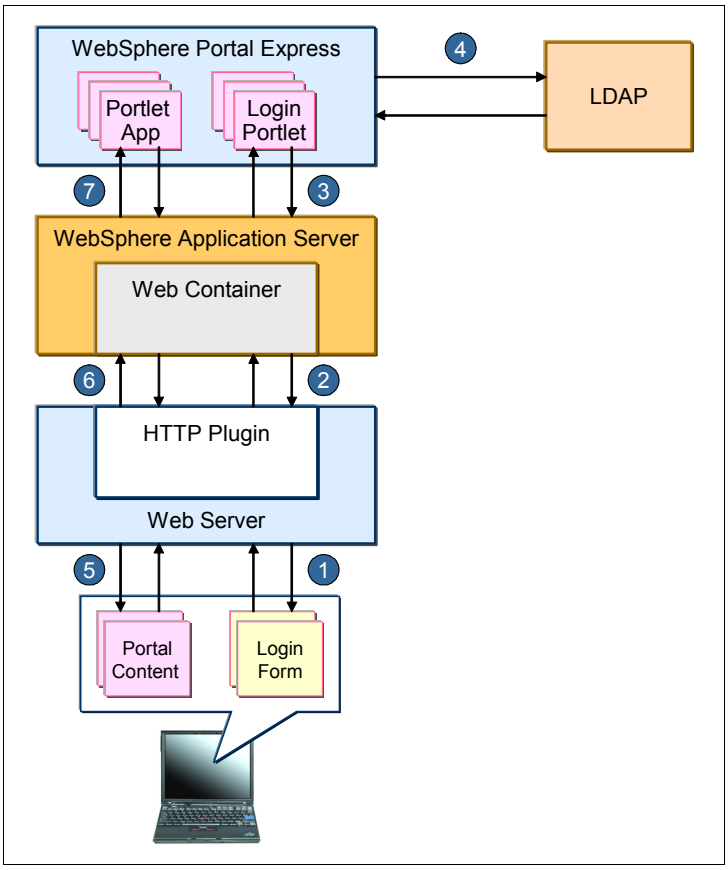


Figure 5-1 Securing your WebSphere Portal environment

To secure the login process only, you have to secure the login data stream between the client Web browser and WebSphere Portal (including the Web server and WebSphere Application Server), and also between WebSphere Portal and your Lightweight Directory Access Protocol (LDAP) server.

If you want to secure the full portal content, you *must* first encrypt the login process (Web server, WebSphere Application Server, WebSphere Portal, and LDAP), and then perform additional configuration steps to secure the whole portal content.

The configuration steps to secure the communication between the client Web browser and the Web server, between the Web server and WebSphere Application Server, and between WebSphere Portal and the LDAP Server are the same in all cases. Only the configuration steps for WebSphere Portal are different, depending on what you want to secure (login process only or whole portal content).

5.1 SSL between WebSphere Portal Express and the LDAP server

This section describes how to configure SSL between WebSphere Portal Express and the LDAP server to make sure that any traffic between those two components is encrypted and secured. This single step is not sufficient by itself to fully secure the user credentials. You need to implement SSL between WebSphere Portal Express and the client Web browser, at least for the login process, to ensure that user credentials are secured from one end to the other.

Enabling SSL between WebSphere Portal and the LDAP server requires these actions:

- 5.1.1, “Certificate management” on page 155
  - “Creating a certificate store” on page 156
  - “Creating a Local Certificate Authority” on page 158.
  - “Exporting the Local Certificate Authority public certificate” on page 165
  - “Importing the Local Certificate Authority public certificate into WebSphere Application Server Java trust store” on page 168
  - “Importing the Local Certificate Authority public certificate into the WebSphere Application Server trust store” on page 169
- 5.1.2, “Enabling SSL for the LDAP server” on page 170
  - “Creating the key certificate for IBM Directory Server” on page 171
  - “Enabling SSL connections for the IBM Directory Server” on page 179
- 5.1.3, “Enabling SSL for WebSphere Portal Express” on page 181

5.1.1 Certificate management

Note: The trust stores, key stores, and their passwords that we use in this chapter are the default ones included with WebSphere Application Server. If you decide to use different stores, see the WebSphere Application Server for OS/400 V6 Information Center at:

http://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/topic/com.ibm.Websphere.iseries.doc/info/ae/ae/tsec_sslrep.html

Creating a certificate store

Perform the following steps to create a certificate store:

1. Open a Web browser and type the following address: `http://your_system:2001/`. Enter your sign on credentials as required, and then click **Digital Certificate Manager** (Figure 5-2).

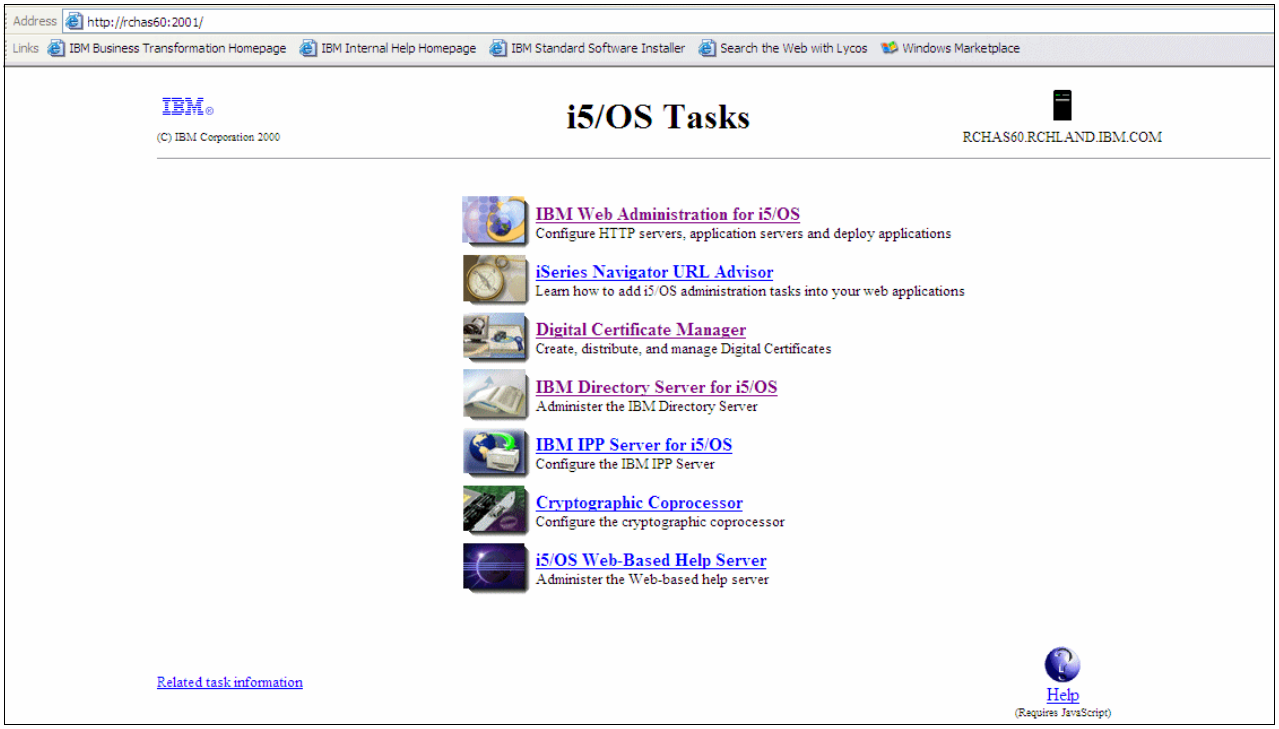

Address http://rchas60:2001/
Links IBM Business Transformation Homepage
IBM Internal Help Homepage
IBM Standard Software Installer
Search the Web with Lycos
Windows Marketplace
IBM
(C) IBM Corporation 2000
i5/OS Tasks
RCHAS60.RCHLAND.IBM.COM
IBM Web Administration for i5/OS
Configure HTTP servers, application servers and deploy applications
iSeries Navigator URL Advisor
Learn how to add i5/OS administration tasks into your web applications
Digital Certificate Manager
Create, distribute, and manage Digital Certificates
IBM Directory Server for i5/OS
Administer the IBM Directory Server
IBM IPP Server for i5/OS
Configure the IBM IPP Server
Cryptographic Coprocessor
Configure the cryptographic coprocessor
i5/OS Web-Based Help Server
Administer the Web-based help server
Related task information
Help
(Requires JavaScript)

Figure 5-2 Accessing the Digital Certificate Manager

2. On the Digital Certificate Manager window, click **Create New Certificate Store** in the left navigation pane (Figure 5-3).

Digital Certificate Manager
Select a Certificate Store
Expand All
Collapse All
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage User Certificates
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1 (C) Copyright IBM Corporation 1997, 2005
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM
GENUINE RSA ENCRYPTION ENGINE
Contains software from RSA Data Security, Inc.
Get Started

Figure 5-3 Creating a new certificate store

3. Select ***SYSTEM** and click **Continue** (Figure 5-4). If *SYSTEM does not appear in the list, then this certificate store already exists on the system and you can go to “Creating a Local Certificate Authority” on page 158.

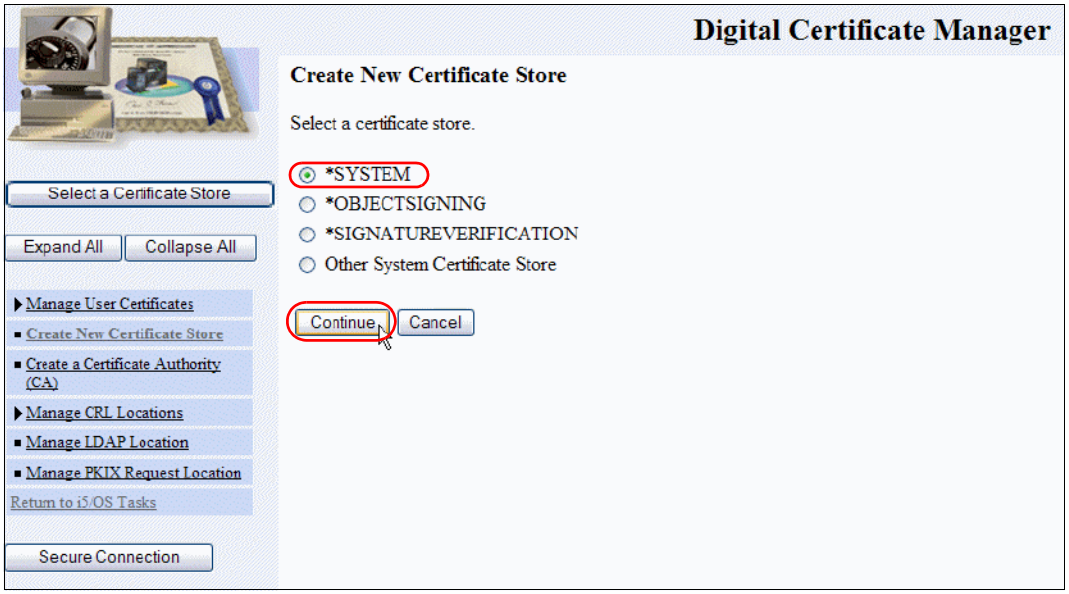


*Figure 5-4 Creating a *SYSTEM certificate store*

4. Select **No - Do not create a certificate in the certificate store** and click **Continue** (Figure 5-5).

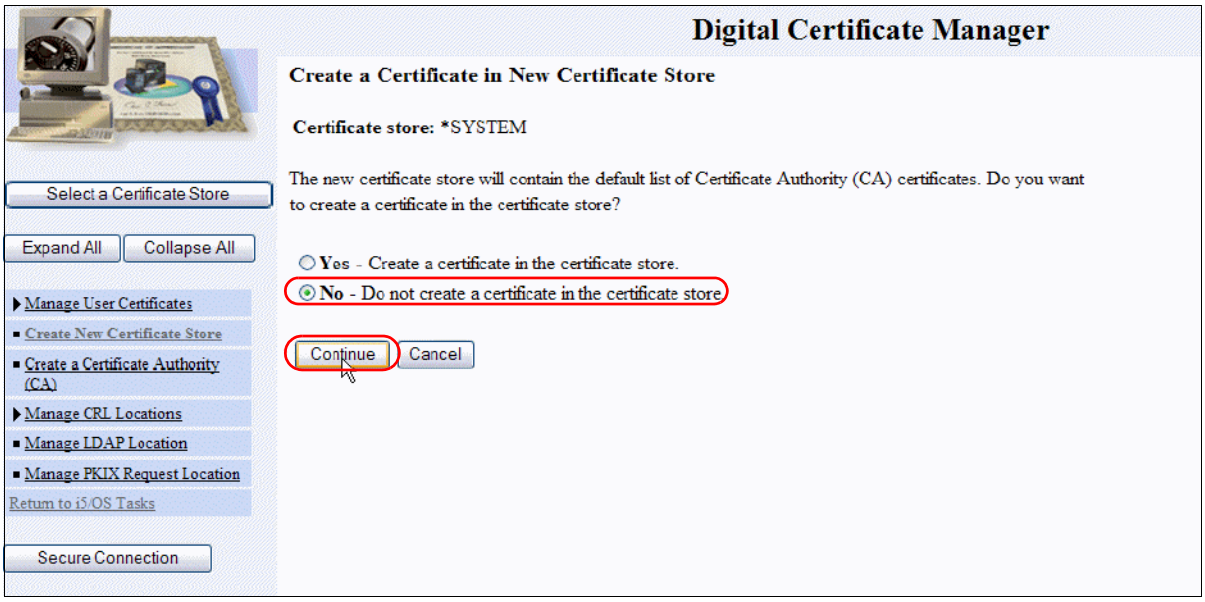

Digital Certificate Manager
Create a Certificate in New Certificate Store
Certificate store: *SYSTEM
The new certificate store will contain the default list of Certificate Authority (CA) certificates. Do you want to create a certificate in the certificate store?
Yes - Create a certificate in the certificate store.
No - Do not create a certificate in the certificate store
Continue
Cancel
Select a Certificate Store
Expand All
Collapse All
Manage User Certificates
Create New Certificate Store
Create a Certificate Authority (CA)
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection

Figure 5-5 Creating an empty certificate store

5. Set the password for the certificate store and click **Continue** (Figure 5-6).

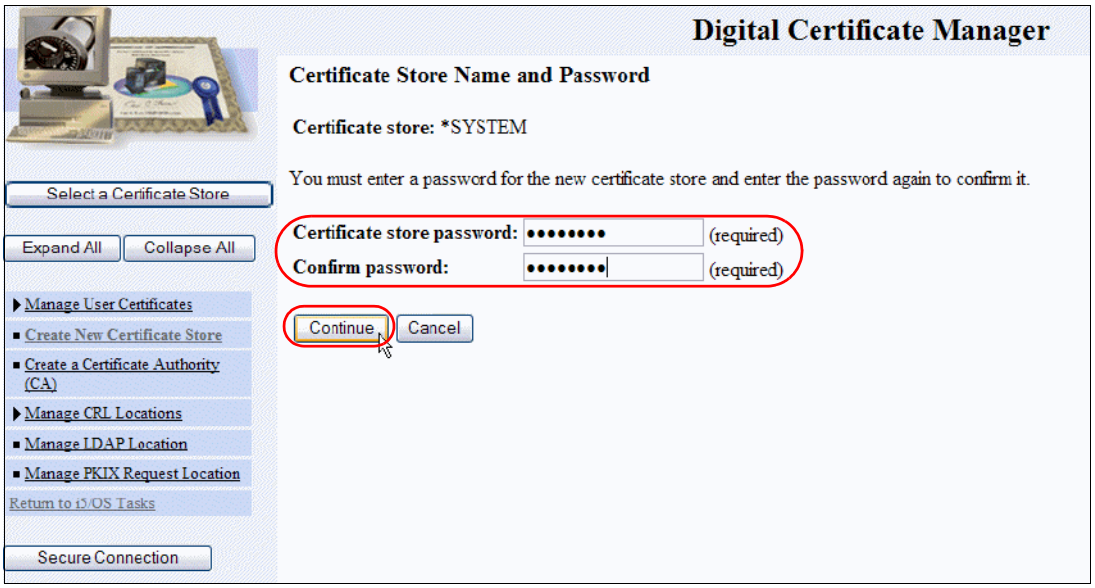


Figure 5-6 Setting the certificate store password

6. A message is shown indicating the location of the certificate store (Figure 5-7). Click **OK**.

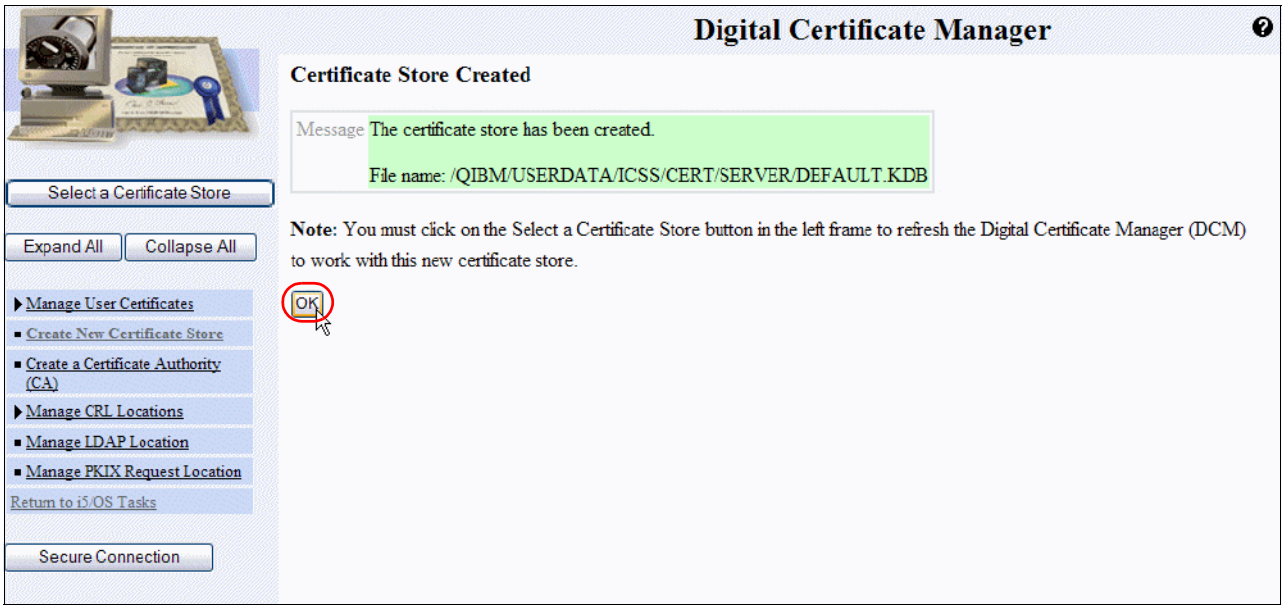

Digital Certificate Manager
Certificate Store Created
Message
The certificate store has been created.
File name: /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
Note: You must click on the Select a Certificate Store button in the left frame to refresh the Digital Certificate Manager (DCM) to work with this new certificate store.
Select a Certificate Store
Expand All
Collapse All
OK
Manage User Certificates
Create New Certificate Store
Create a Certificate Authority (CA)
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection

Figure 5-7 Certificate store location

Creating a Local Certificate Authority

Perform the following steps to create a local Certificate Authority (CA):

1. Log in to Digital Certificate Manager (refer to “Creating a certificate store” on page 156 to access Digital Certificate Manager).

2. On the Digital Certificate Manager window, click **Select a Certificate Store** in the left navigation pane (Figure 5-8).

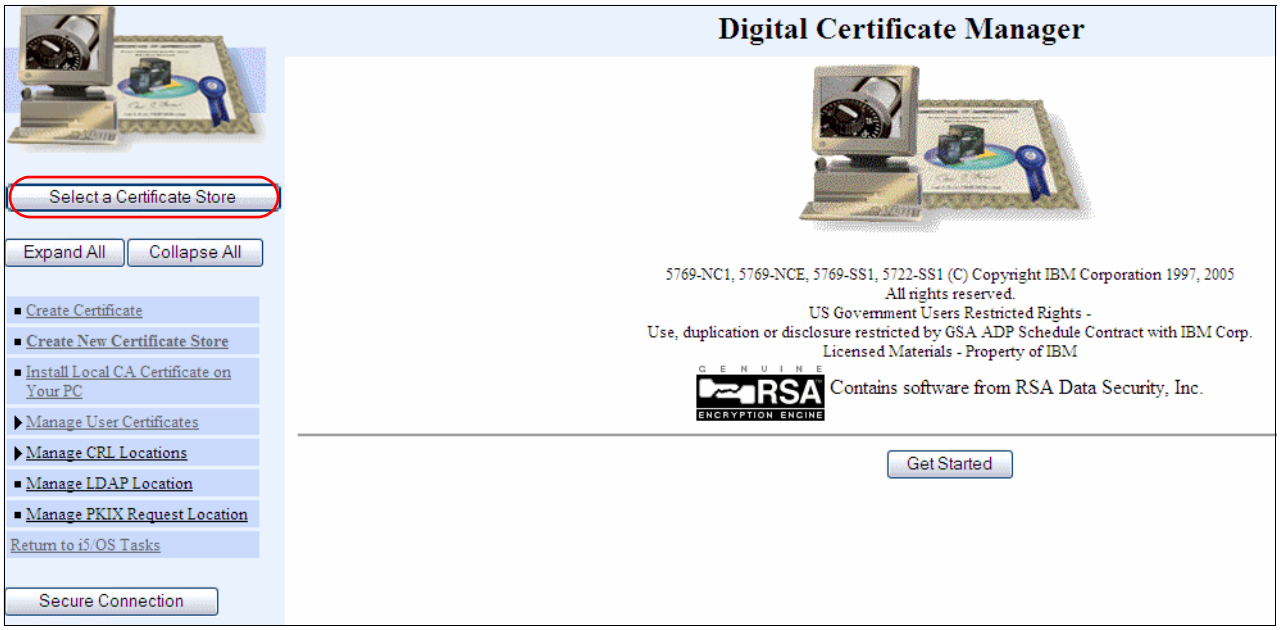

Digital Certificate Manager
Select a Certificate Store
Expand All
Collapse All
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage User Certificates
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1 (C) Copyright IBM Corporation 1997, 2005
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM
Contains software from RSA Data Security, Inc.
Get Started

Figure 5-8 Selecting a certificate store

3. Select ***SYSTEM** and click **Continue** (Figure 5-9).

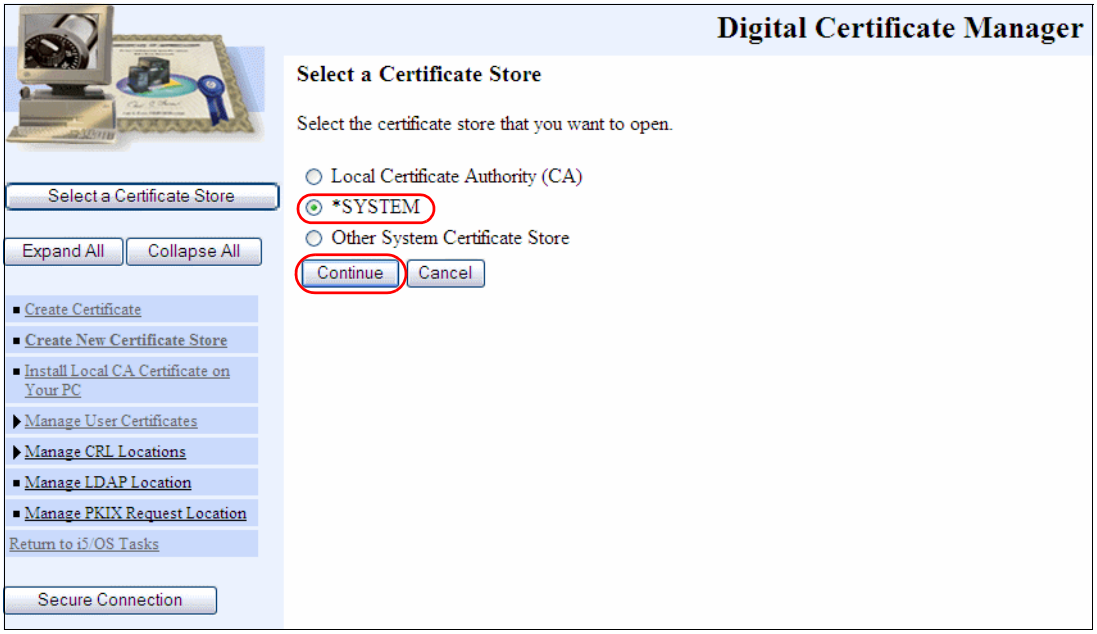


*Figure 5-9 Selecting *SYSTEM certificate store*

4. Enter the password for the *SYSTEM certificate store and click **Continue** (Figure 5-10).

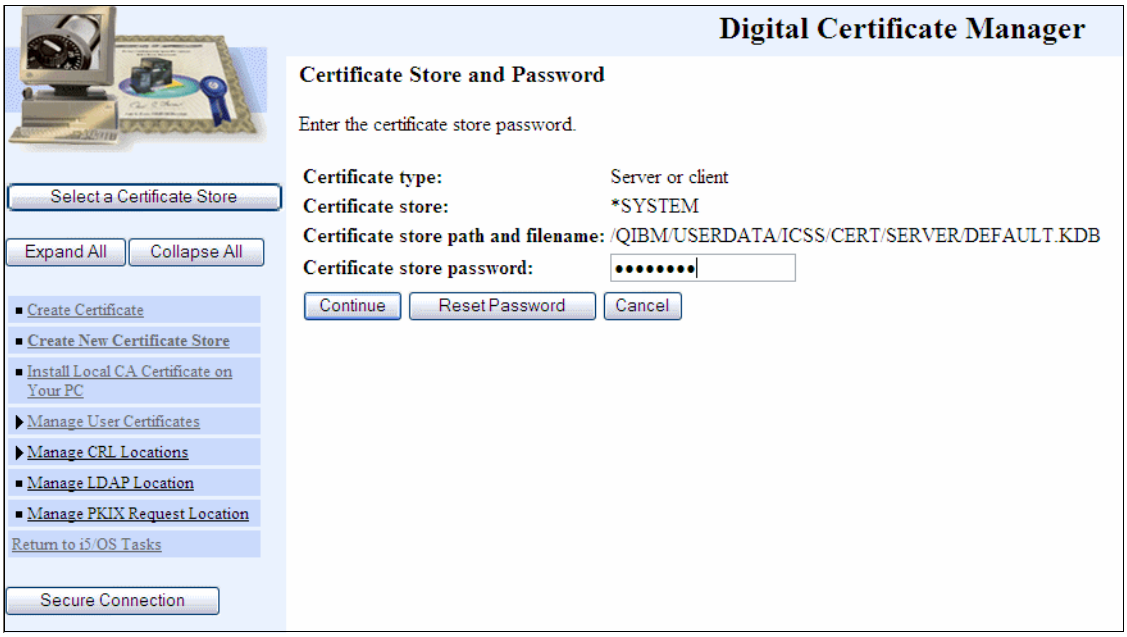


*Figure 5-10 Entering the *SYSTEM certificate store password*

5. Information is displayed about the current certificate store. In the left navigation pane, click **Create A Certificate Authority (CA)** (Figure 5-11). If this link does not appear in the left navigation pane, there is already an existing Certificate Authority in this certificate store. Then, go to “Exporting the Local Certificate Authority public certificate” on page 165.

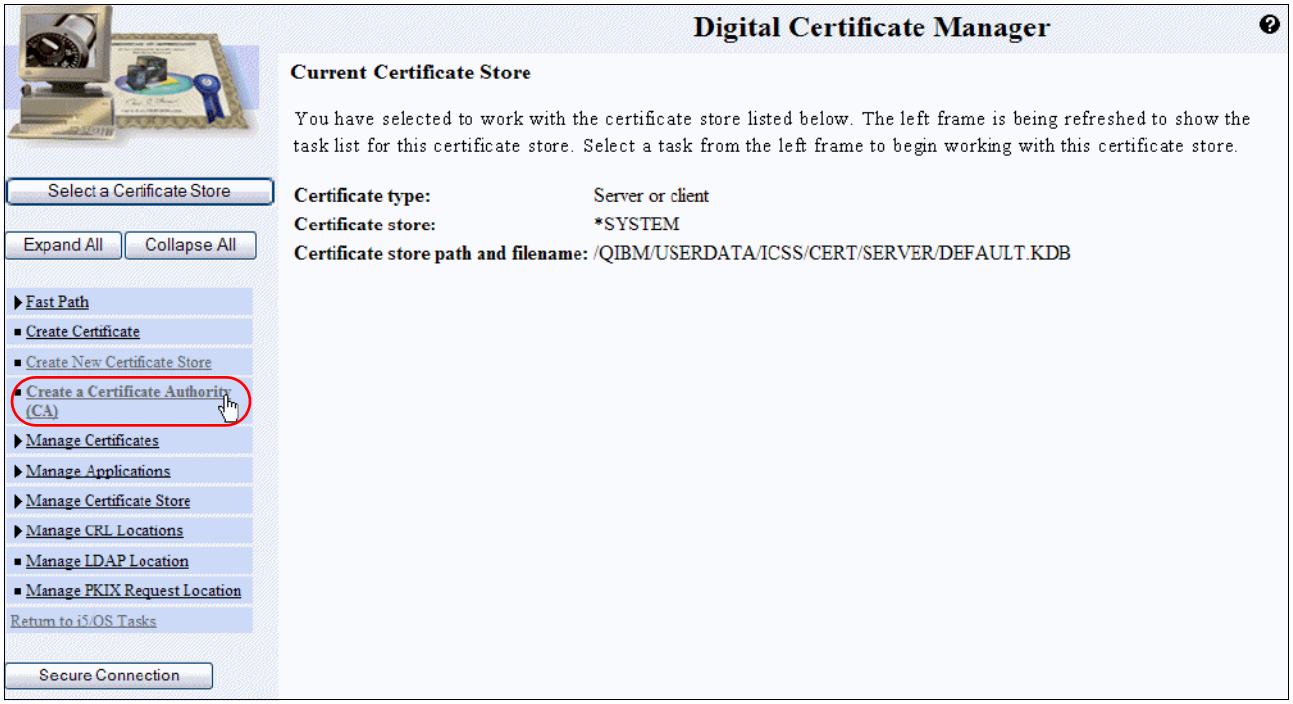

Digital Certificate Manager
Current Certificate Store
You have selected to work with the certificate store listed below. The left frame is being refreshed to show the task list for this certificate store. Select a task from the left frame to begin working with this certificate store.
Certificate type: Server or client
Certificate store: *SYSTEM
Certificate store path and filename: /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
Select a Cerificate Store
Expand All
Collapse All
Fast Path
Create Certificate
Create New Certificate Store
Create a Certificate Authority (CA)
Manage Certificates
Manage Applications
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection

Figure 5-11 Creating a local Certificate Authority

6. You are then presented with a form requesting the local CA information. Complete the required fields and click **Continue** (Figure 5-12).

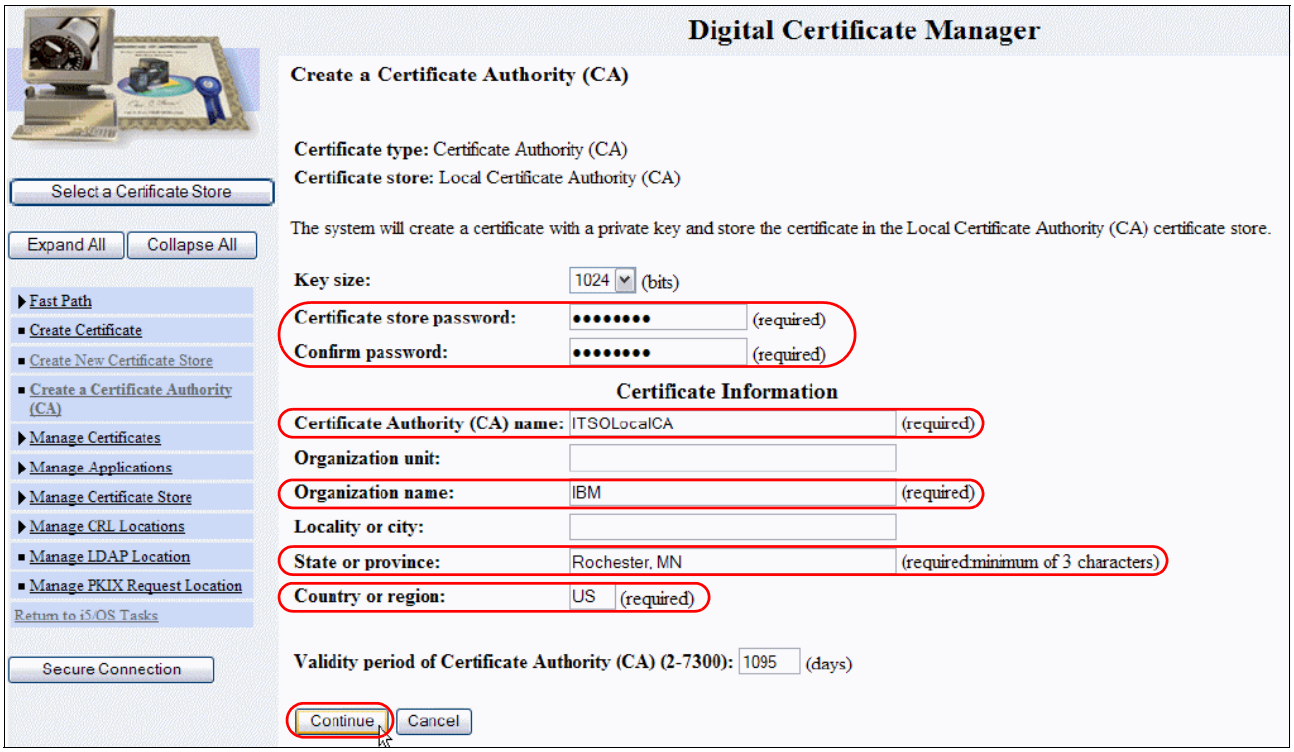

Digital Certificate Manager
Create a Certificate Authority (CA)
Certificate type: Certificate Authority (CA)
Certificate store: Local Certificate Authority (CA)
The system will create a certificate with a private key and store the certificate in the Local Certificate Authority (CA) certificate store.
Key size: 1024 (bits)
Certificate store password: (required)
Confirm password: (required)
Certificate Information
Certificate Authority (CA) name: ITSOLocalCA (required)
Organization unit:
Organization name: IBM (required)
Locality or city:
State or province: Rochester, MN (required:minimum of 3 characters)
Country or region: US (required)
Validity period of Certificate Authority (CA) (2-7300): 1095 (days)
Continue
Cancel
Select a Cerificate Store
Expand All
Collapse All
Fast Path
Create Certificate
Create New Certificate Store
Create a Certificate Authority (CA)
Manage Certificates
Manage Applications
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection

Figure 5-12 Local Certificate Authority information

7. You are offered the opportunity to install the local CA into your Web browser. Do *not* install the local CA and click **Continue** (Figure 5-13).

Digital Certificate Manager
Install Local CA Certificate
Certificate type: Certificate Authority (CA)
Certificate store: Local Certificate Authority (CA)
A certificate for your Certificate Authority (CA) was created and stored in the local Certificate Authority (CA) certificate store.
You must install the Certificate Authority (CA) certificate in your browser so the browser can verify certificates that your CA issues. Click the following link to install the certificate in your browser. Your web browser will display several windows to help you complete the installation of the certificate.
Install certificate
After installing the certificate, select Continue so you can provide the policy data that will be used for signing and issuing certificates with this Certificate Authority (CA).
Continue
Cancel
Select a Cerificate Store
Expand All
Collapse All
Fast Path
Create Certificate
Create New Certificate Store
Create a Certificate Authority (CA)
Manage Certificates
Manage Applications
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection

Figure 5-13 Do not install the local CA into your Web browser

8. You are shown the policy data about the local CA. You might want to change the validity period of certificates issued by the local CA. The default is 365 days. Click **Continue** (Figure 5-14).

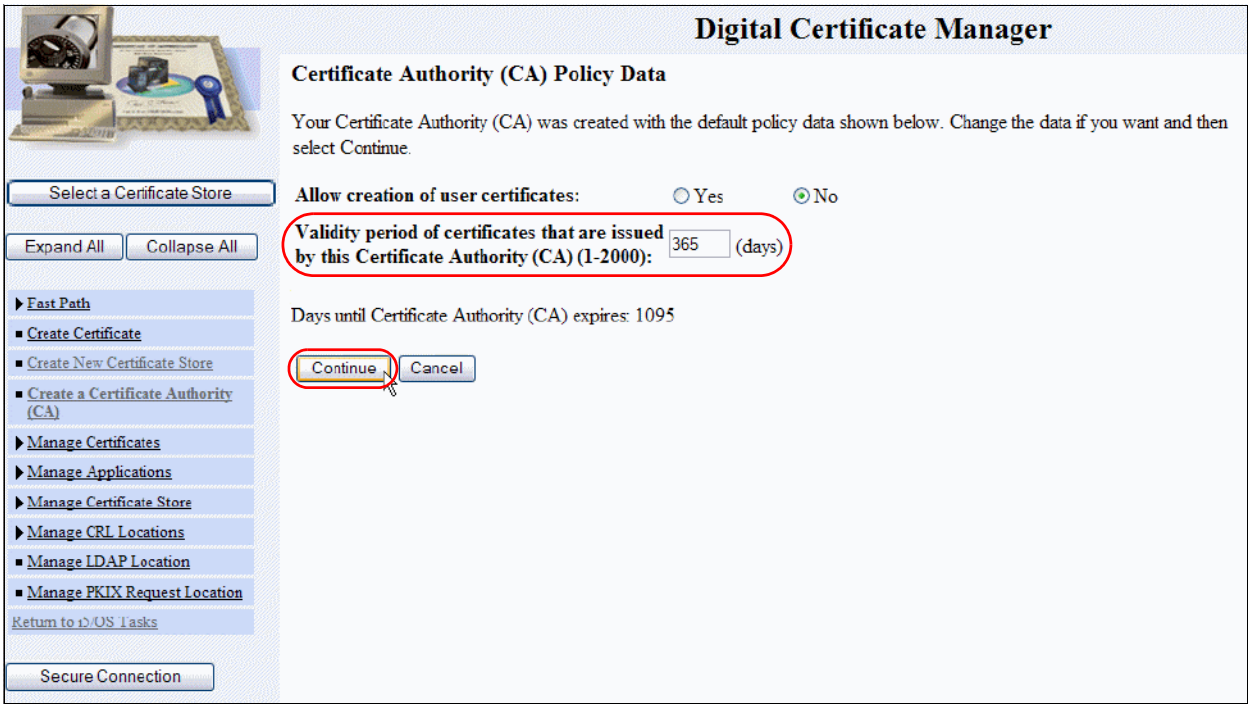


Figure 5-14 Entering policy data for the local Certificate Authority

9. You are then presented with a list of applications that can trust the local CA. Do *not* select any applications. Click **Continue** (Figure 5-15).

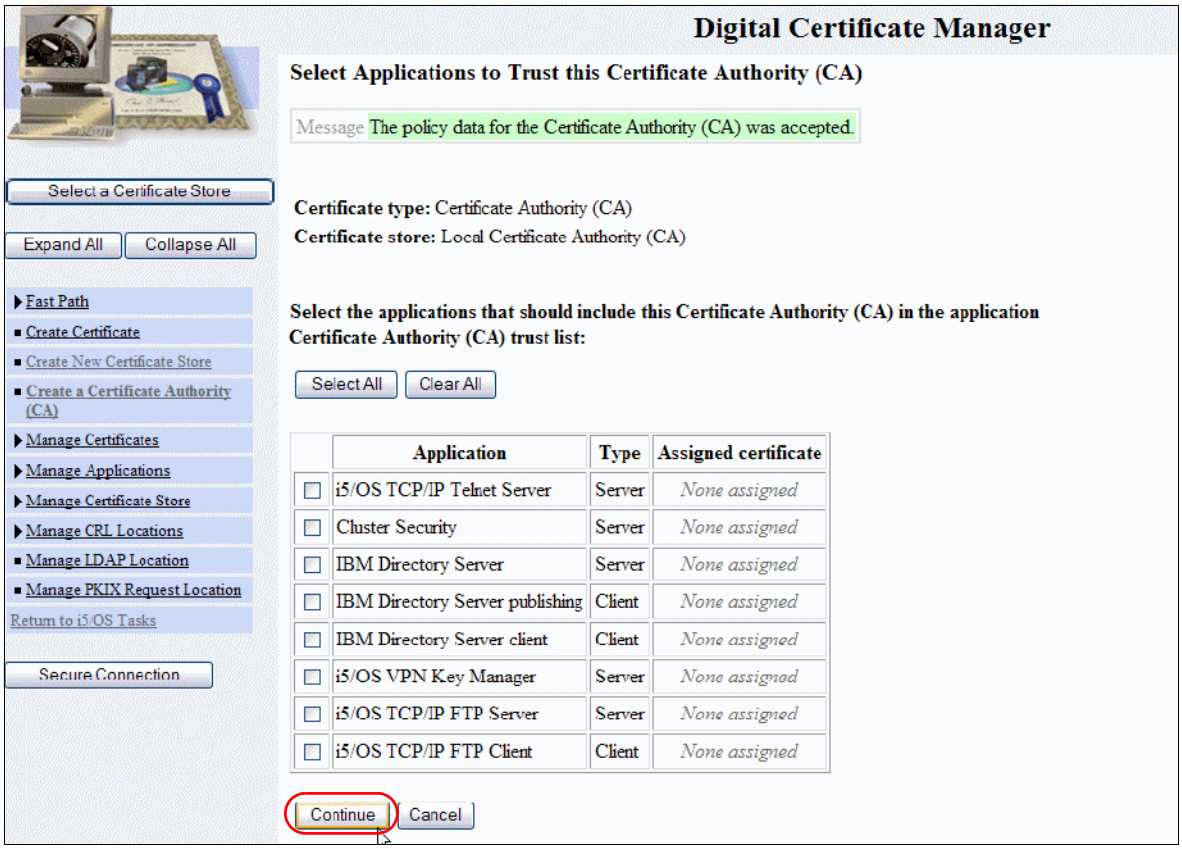


Figure 5-15 Do not select any applications to trust the local CA

10. The local CA is now created. Click **Cancel** to complete this section (Figure 5-16).

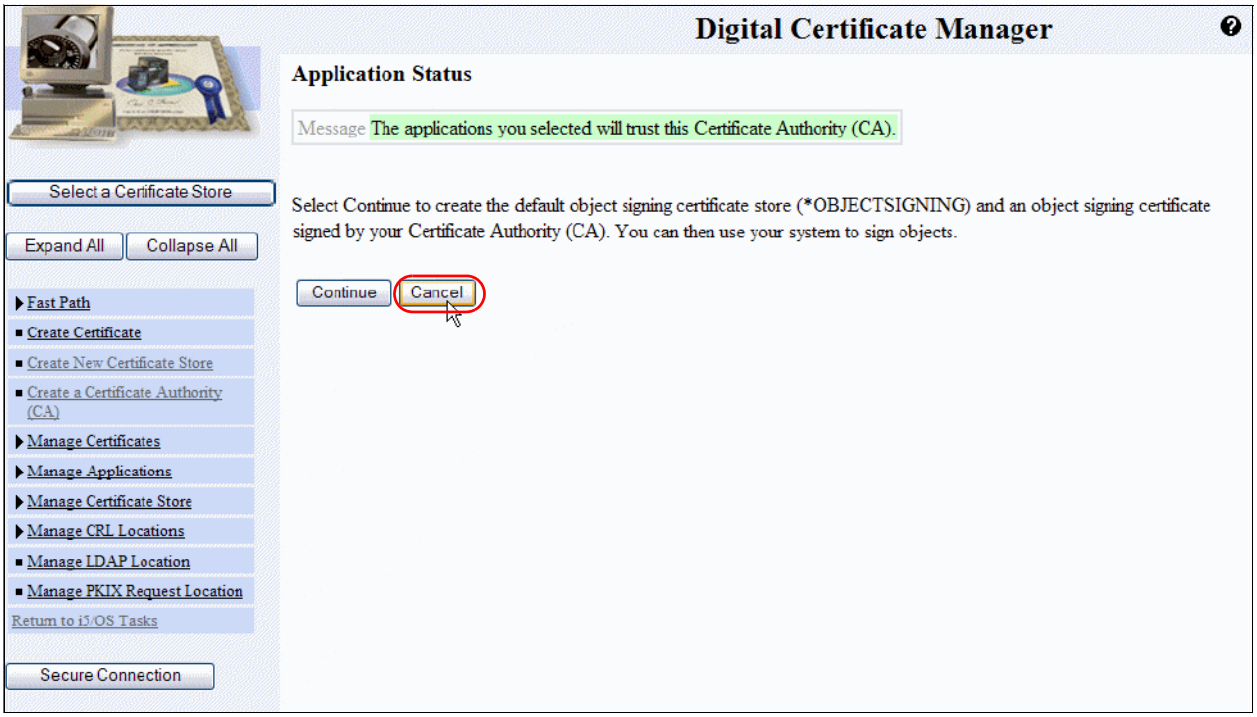

Digital Certificate Manager
Application Status
Message The applications you selected will trust this Certificate Authority (CA).
Select Continue to create the default object signing certificate store (*OBJECTSIGNING) and an object signing certificate signed by your Certificate Authority (CA). You can then use your system to sign objects.
Continue
Cancel
Select a Certificate Store
Expand All
Collapse All
Fast Path
Create Certificate
Create New Certificate Store
Create a Certificate Authority (CA)
Manage Certificates
Manage Applications
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection

Figure 5-16 Local Certificate Authority successfully created

Exporting the Local Certificate Authority public certificate

Perform the following steps to export the Local Certificate Authority public certificate:

1. Log in to the Digital Certificate Manager (see “Creating a certificate store” on page 156 to access the Digital Certificate Manager).

2. In the left navigation pane of the Digital Certificate Manager window, click **Install Local CA Certificate on Your PC** (Figure 5-17).

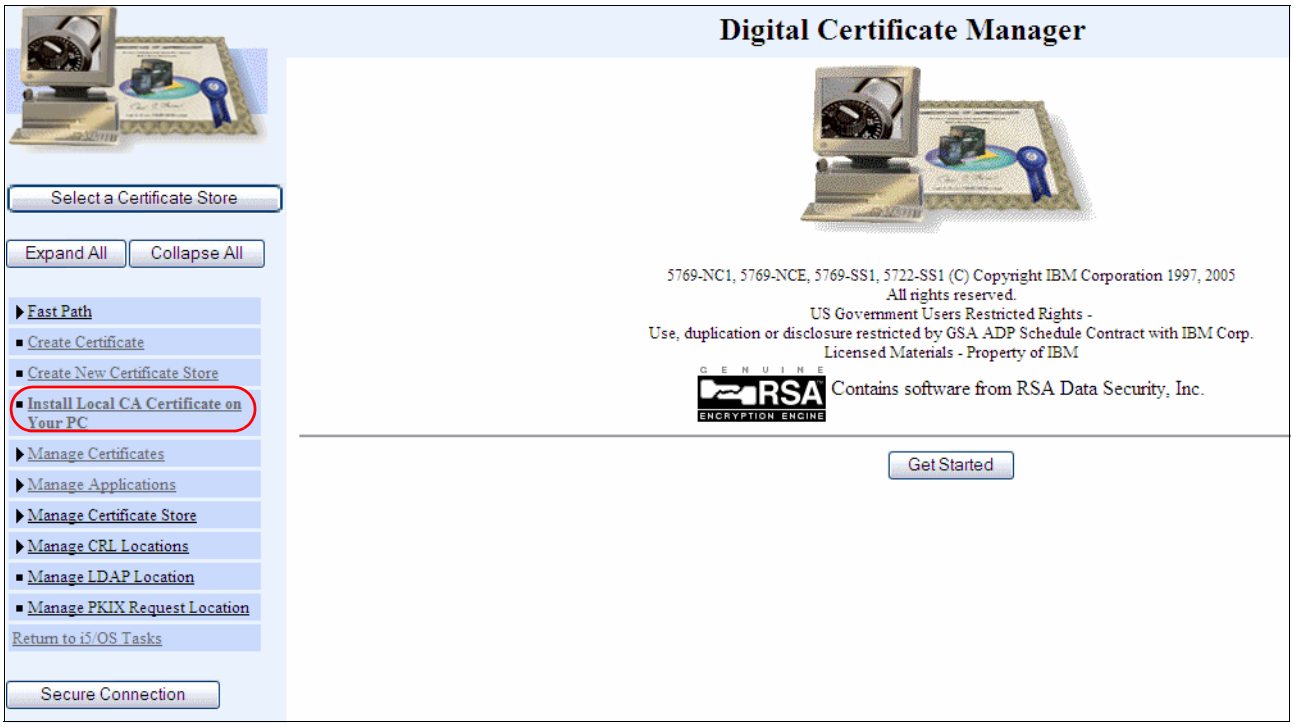

Digital Certificate Manager
Select a Certificate Store
Expand All
Collapse All
Fast Path
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
Manage Applications
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1 (C) Copyright IBM Corporation 1997, 2005
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM
Contains software from RSA Data Security, Inc.
Get Started

Figure 5-17 Exporting Local CA public certificate

3. Click **Copy and paste certificate** (Figure 5-18).

Digital Certificate Manager
Select a Certificate Store
Expand All
Collapse All
Fast Path
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
Manage Applications
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
Install Local CA Certificate on Your PC
To install (receive) the certificate on your browser:
Click the following link to install the certificate in your browser. Your web browser will display several windows to help you complete the installation of the certificate.
Install certificate
To copy and paste the certificate to a file on your PC:
If you need the Certificate Authority (CA) certificate for a non-browser application such as Client Access Express or IBM Personal Communications, choose the Copy and paste certificate link. Use the online help provided here and in the appropriate application for information about working with your certificate file. Click the following link to copy and paste the certificate into a file on your PC.
Copy and paste certificate
OK

Figure 5-18 Extracting the Local CA public certificate

4. The certificate is then displayed (Figure 5-19).

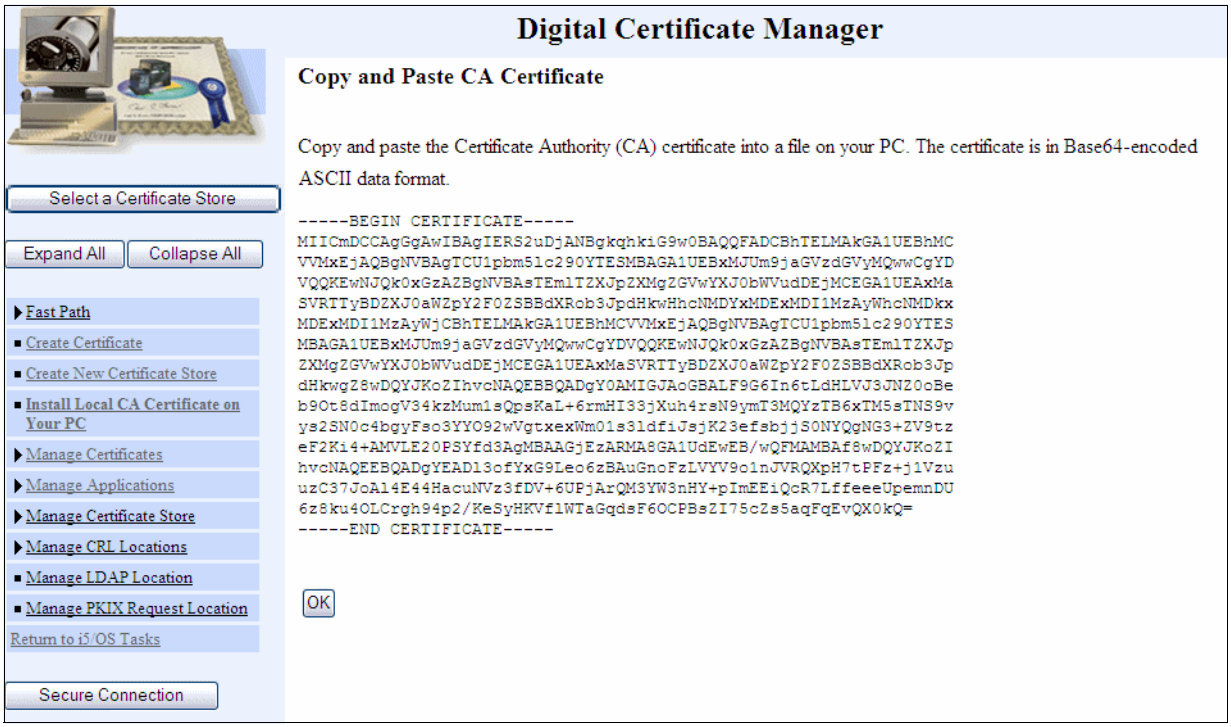


Figure 5-19 Local CA public certificate

5. Copy and paste the certificate into a text editor of your choice (for example, Notepad or WordPad) and save this file on your desktop (Figure 5-20). You need to include the lines containing BEGIN CERTIFICATE and END CERTIFICATE. In our example, we saved the file under the name of `ITSOCertificate Authority.txt`.

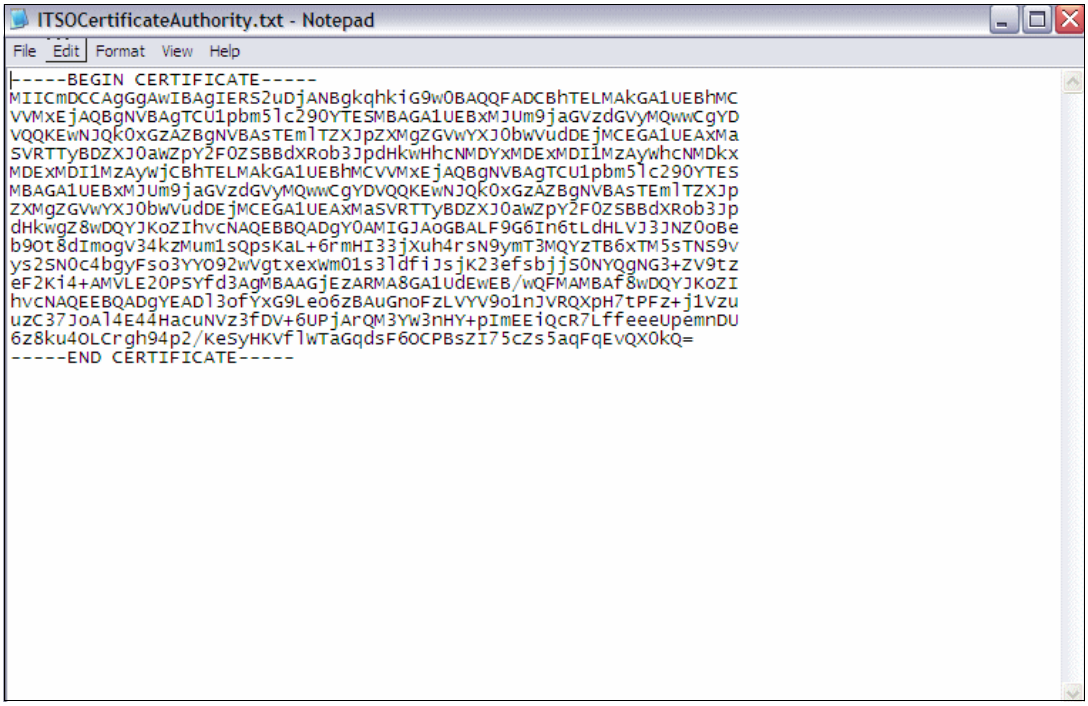


Figure 5-20 Copying the Local CA certificate to a text editor

6. The Local CA public certificate is now available on your desktop. To import it into the WebSphere Application Server trust stores, you have to transfer it to the i5/OS integrated file system, using one the following methods:
   - Use FTP.
   - Copy and transfer using the iSeries Navigator.
   - Copy and transfer using a mapped drive in Windows Explorer.
   - In our example, we copied the certificate in the i5/OS integrated file system to the directory of `/tmp`.

Importing the Local Certificate Authority public certificate into WebSphere Application Server Java trust store

Note: Perform this step only once for your system. The WebSphere Application Server Java trust store password is case-sensitive.

The steps to import the Local Certificate Authority public certificate into WebSphere Application Server Java trust store are:

1. Log in to a 5250 emulation session.
2. Start the Qshell environment using the i5/OS CL command of Start Qshell (STRQSH).
3. Type the following command:

   `/QIBM/ProdData/Java400/jdk14/bin/keytool -import -file` *`LCA_certificate_name`* `-keystore /QIBM/ProdData/Java400/jdk14/lib/security/cacerts -alias "`*`alias_name`*`" -trustcacerts`

   The *LCA_certificate_name* is the fully qualified integrated file system name of the Local CA public certificate. In our example, *LCA_certificate_name* has the value `/tmp/ITSOCertificateAuthority.txt`.

   The *alias_name* is an alias that is used to identify the certificate in the store. In our example, we gave it the value of *ITSOSelfSigned.*

4. You are then prompted for the password of the keystore. If you are using the default keystore, the default password is `changeit`. You are asked if you want to trust this certificate, and the answer is `yes` (Figure 5-21).

```
                                QSH Command Entry

  $
> /QIBM/ProdData/Java400/jdk14/bin/keytool -import -file
/tmp/ITSOCertificateAuthority.txt -keystore
/QIBM/ProdData/Java400/jdk14/lib/security/cacerts -alias "ITSOSelfSigned"
-trustcacerts
 Enter keystore password:
 > changeit
   Owner: CN=ITSO Certificate Authority, OU=iSeries department, O=IBM,
L=Rochester, ST=Minnesota, C=US
   Issuer: CN=ITSO Certificate Authority, OU=iSeries department, O=IBM,
L=Rochester, ST=Minnesota, C=US
   Serial number: 452dae0e
   Valid from: Tue Oct 10 21:53:02 CDT 2006 until: Sat Oct 10 21:53:02 CDT 2009
   Certificate fingerprints:
            MD5:  2D:CE:4B:DE:A6:47:22:1F:90:59:E9:89:F5:06:8F:11
            SHA1: 7F:B9:B4:A1:AE:E4:27:16:1C:65:3A:AD:E1:AF:B6:C2:45:6B:C7:F9
   Trust this certificate? [no]:
 > yes
   Certificate was added to keystore
   $
```

Figure 5-21 Importing the Local CA certificate into WebSphere Application Server Java trust store

Note: You can also use the iKeyman utility shipped with WebSphere Application Server to import the Local CA in the trust store. For more information about the iKeyman utility, see the iSeries Information Center V5R4 at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzatz/51/sec/ikeyman.htm

Importing the Local Certificate Authority public certificate into the WebSphere Application Server trust store

Note: Perform this step for each WebSphere Portal Express profile you want to secure. The WebSphere Application Server trust store password is case-sensitive.

The steps to import the Local Certificate Authority public certificate into the WebSphere Application Server trust store are:

1. Log in to a 5250 emulation session.
2. Start the Qshell environment using the i5/OS CL command of Start Qshell (STRQSH).
3. Type the following command:

   /QIBM/ProdData/Java400/jdk14/bin/keytool -import -file *LCA_certificate_name* -keystore /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_instance*/etc/DummyServerTrustFile.jks -alias “*alias_name*” -trustcacerts

The *LCA_certificate_name* is the fully qualified integrated file system name of the Local CA public certificate. In our example, *LCA_certificate_name* has the value `/tmp/ITSOCertificateAuthority.txt`.

The *alias_name* is an alias that is used to identify the certificate in the store. In our example, we gave it the value of `ITSOSelfSigned`.

4. You are prompted for the password of the keystore. If you are using the default keystore, the default password is `WebAS`. You are asked if you want to trust this certificate; the answer is `yes` (Figure 5-22).

```
                                QSH Command Entry

  $
> /QIBM/ProdData/Java400/jdk14/bin/keytool -import -file
/tmp/ITSOCertificateAuthority.txt -keystore
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WPX6PRF/etc/DummyServerTrus
tFile.jks -alias "ITSOSelfSigned" -trustcacerts
 Enter keystore password:
 > WebAS
   Owner: CN=ITSO Certificate Authority, OU=iSeries department, O=IBM,
L=Rochester, ST=Minnesota, C=US
   Issuer: CN=ITSO Certificate Authority, OU=iSeries department, O=IBM,
L=Rochester, ST=Minnesota, C=US
   Serial number: 452dae0e
   Valid from: Tue Oct 10 21:53:02 CDT 2006 until: Sat Oct 10 21:53:02 CDT 2009
   Certificate fingerprints:
            MD5:  2D:CE:4B:DE:A6:47:22:1F:90:59:E9:89:F5:06:8F:11
            SHA1: 7F:B9:B4:A1:AE:E4:27:16:1C:65:3A:AD:E1:AF:B6:C2:45:6B:C7:F9
   Trust this certificate? [no]:
 > yes
   Certificate was added to keystore
   $
```

Figure 5-22 Importing the Local CA certificate into WebSphere Application Server trust store

Note: You can also use the iKeyman utility shipped with WebSphere Application Server to import the Local CA into the trust store. For more information about the iKeyman utility, see the iSeries Information Center V5R4 at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzatz/51/sec/ikeyman.htm

5.1.2 Enabling SSL for the LDAP server

Note: The steps described in this section assume that you are using the IBM Directory Server as the LDAP server. If you are using a different LDAP server, then see the specific documentation of that directory server.

Creating the key certificate for IBM Directory Server

Perform the following steps to create the key certificate for the IBM Directory Server:

1. Log in to the Digital Certificate Manager (see “Creating a certificate store” on page 156 to access the Digital Certificate Manager).
2. On the Digital Certificate Manager window, click **Select a Certificate Store** (Figure 5-23).

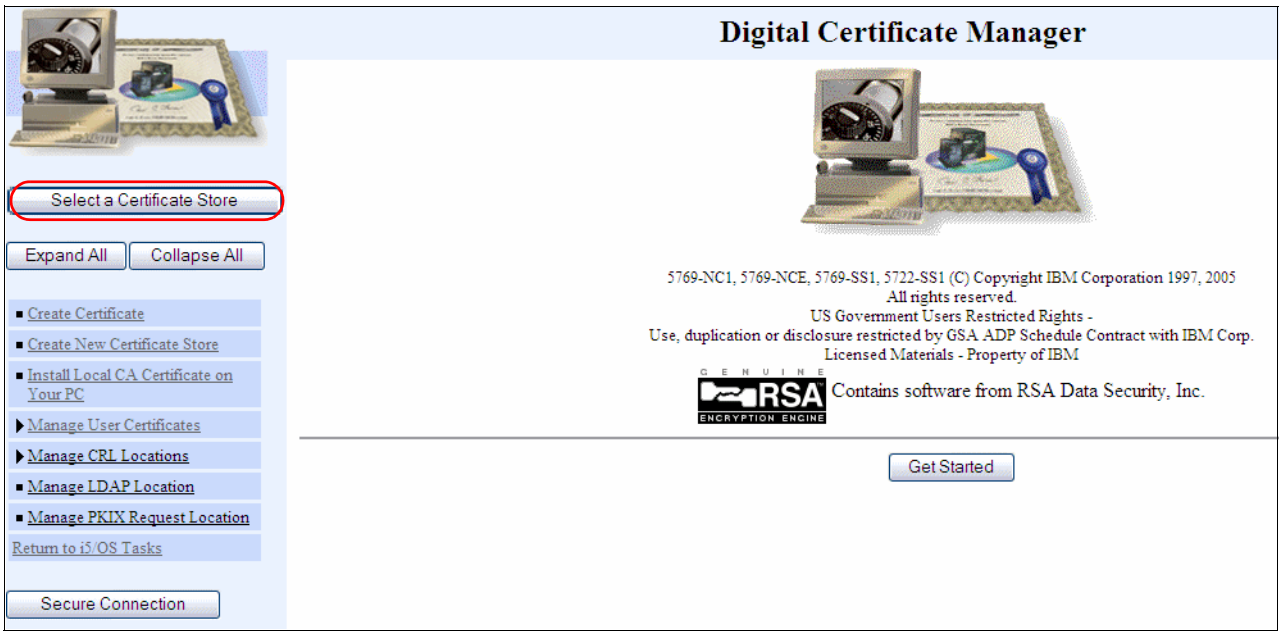

Digital Certificate Manager
Select a Certificate Store
Expand All
Collapse All
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage User Certificates
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1 (C) Copyright IBM Corporation 1997, 2005
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM
Contains software from RSA Data Security, Inc.
Get Started

Figure 5-23 Selecting a certificate store

3. Select ***SYSTEM** and click **Continue** (Figure 5-24).

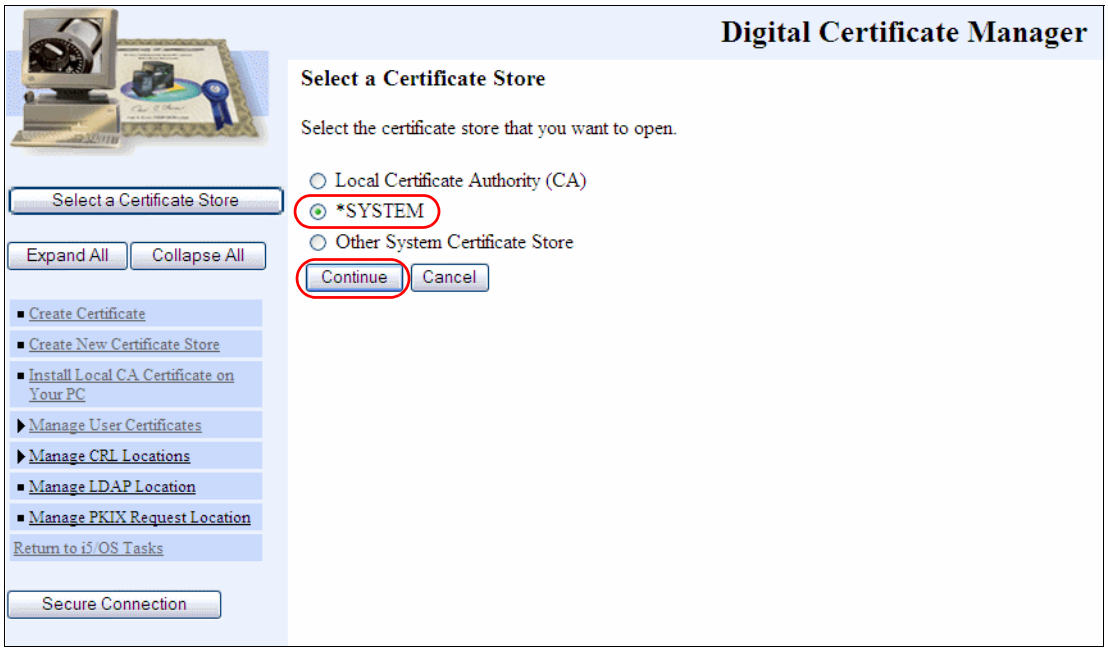


*Figure 5-24 Selecting the *SYSTEM certificate store*

4. The location of the certificate is shown. To access this certificate store, enter its password and click **Continue** (Figure 5-25).

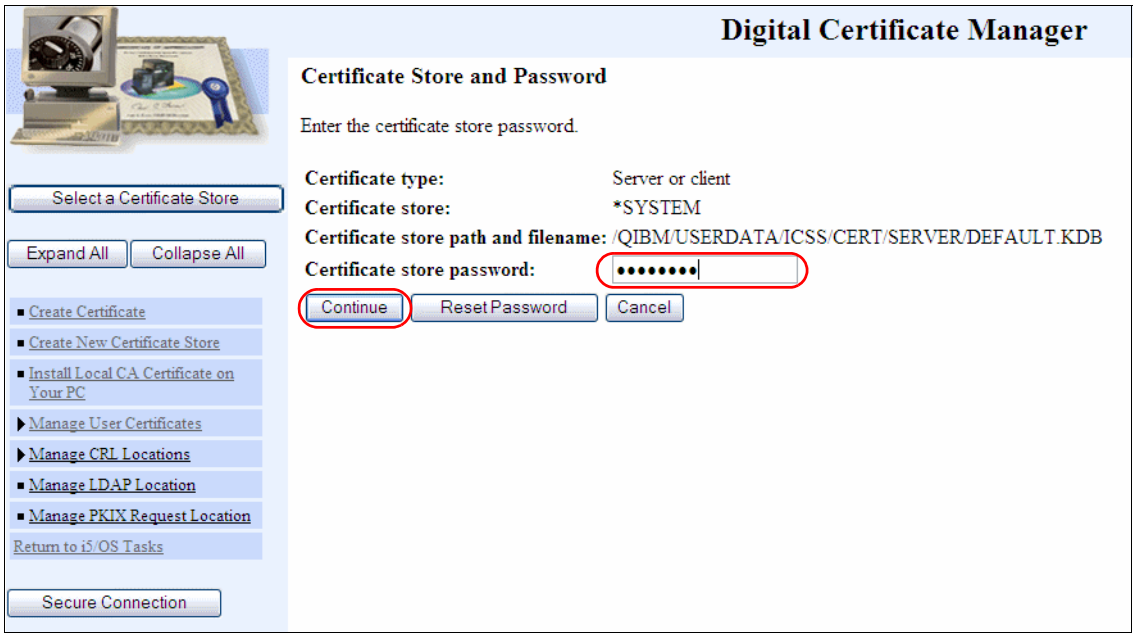


*Figure 5-25 Entering the *SYSTEM certificate store*

5. You are now in the *SYSTEM certificate store. Click **Create Certificate** (Figure 5-26).

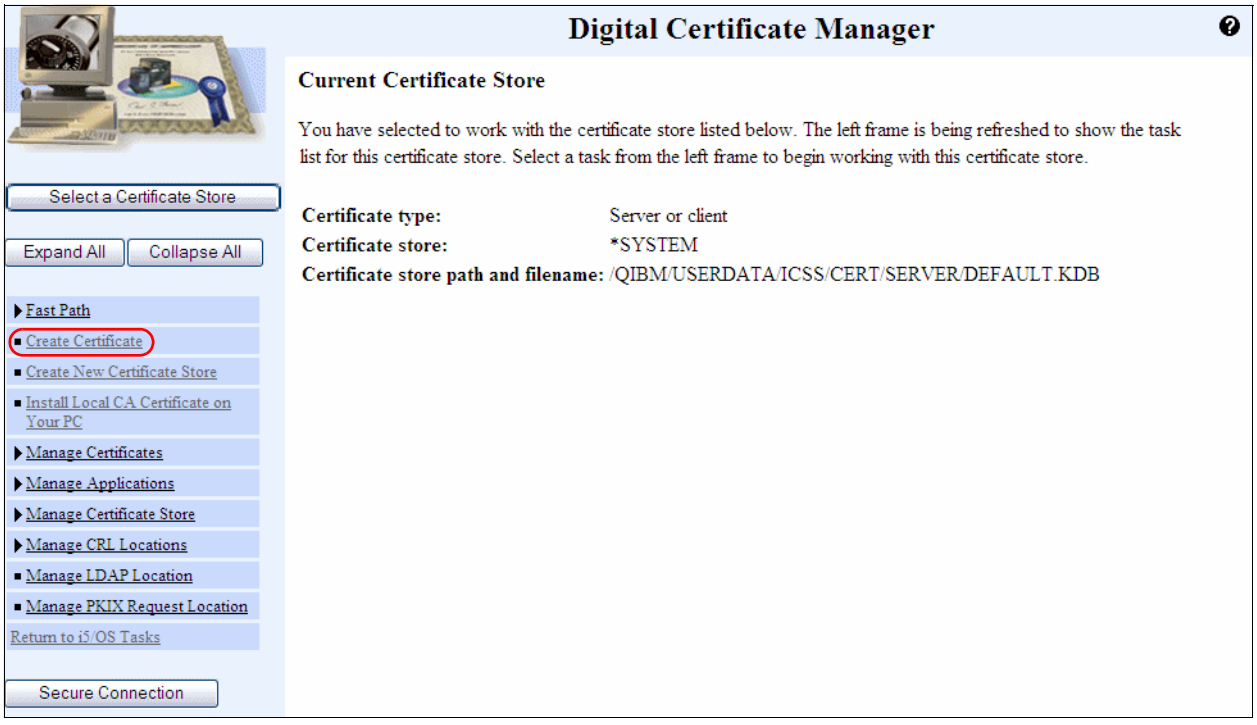

Digital Certificate Manager
Current Certificate Store
You have selected to work with the certificate store listed below. The left frame is being refreshed to show the task list for this certificate store. Select a task from the left frame to begin working with this certificate store.
Certificate type: Server or client
Certificate store: *SYSTEM
Certificate store path and filename: /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
Select a Certificate Store
Expand All
Collapse All
Fast Path
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
Manage Applications
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection

Figure 5-26 Creating a new certificate

6. Select **Server or client certificate** and click **Continue** (Figure 5-27).

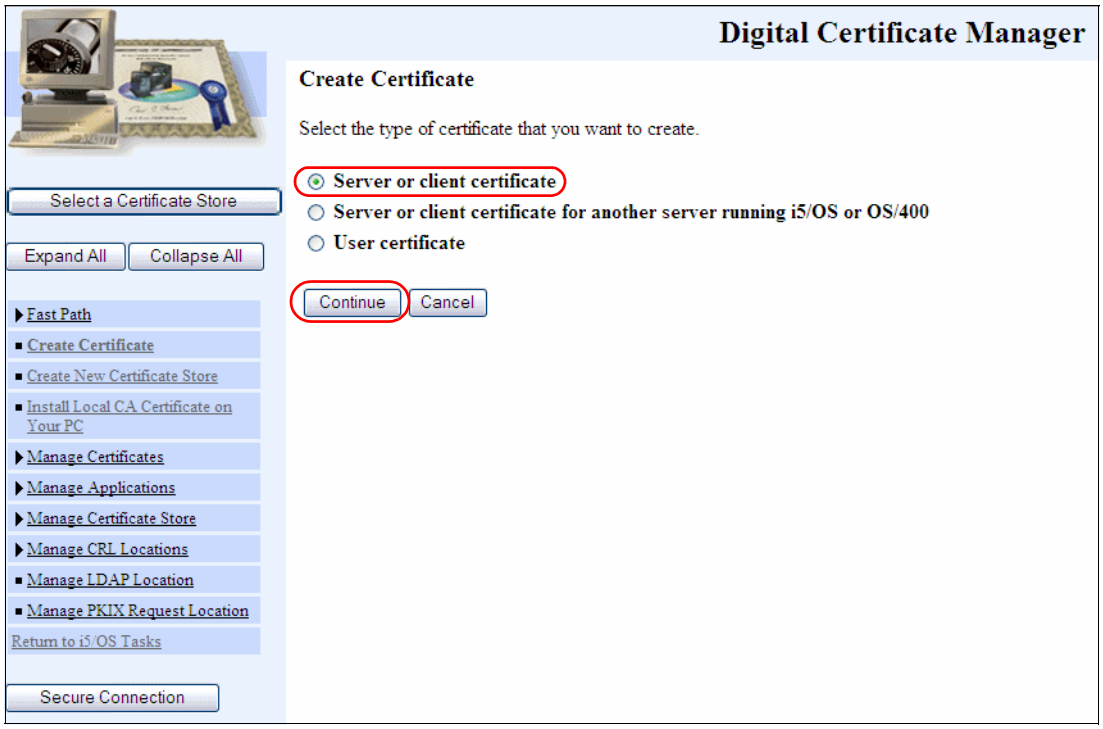


Figure 5-27 Creating a new server certificate

7. A list of Certificate Authorities that can sign certificates is presented. Select **Local Certificate Authority (CA)** and click **Continue** (Figure 5-28).

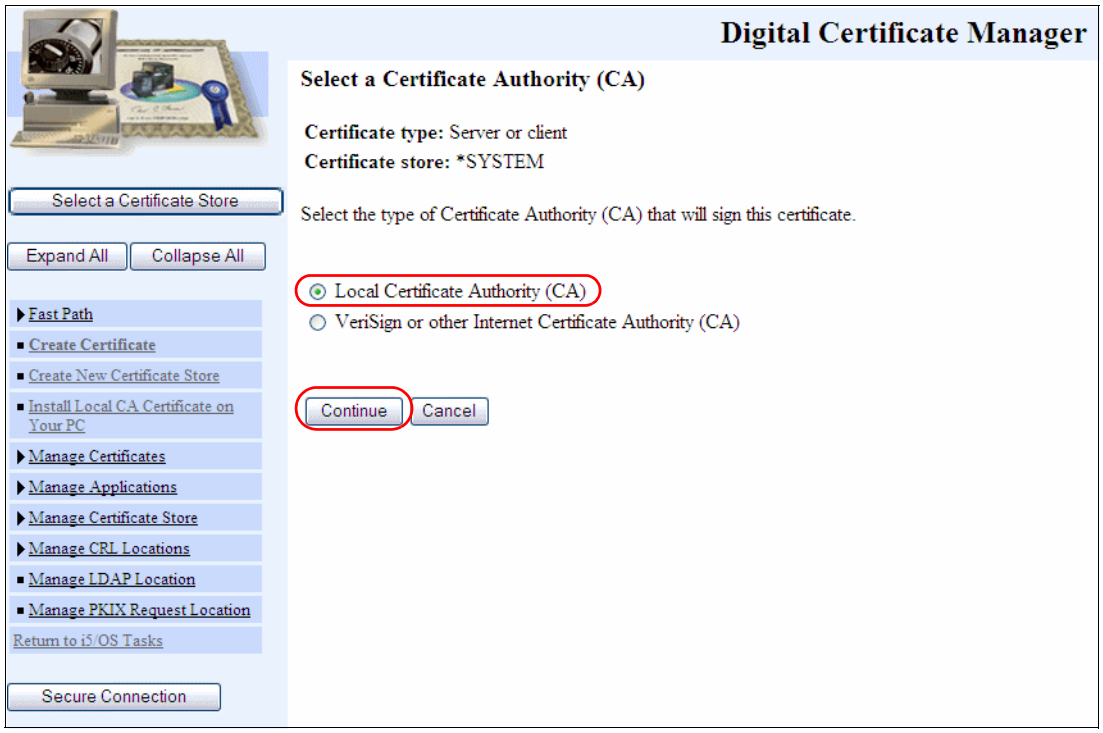


Figure 5-28 Selecting the Certificate Authority

8. You are now presented with a window requesting the certificate information. Enter at least the required information and click **Continue** (Figure 5-29).

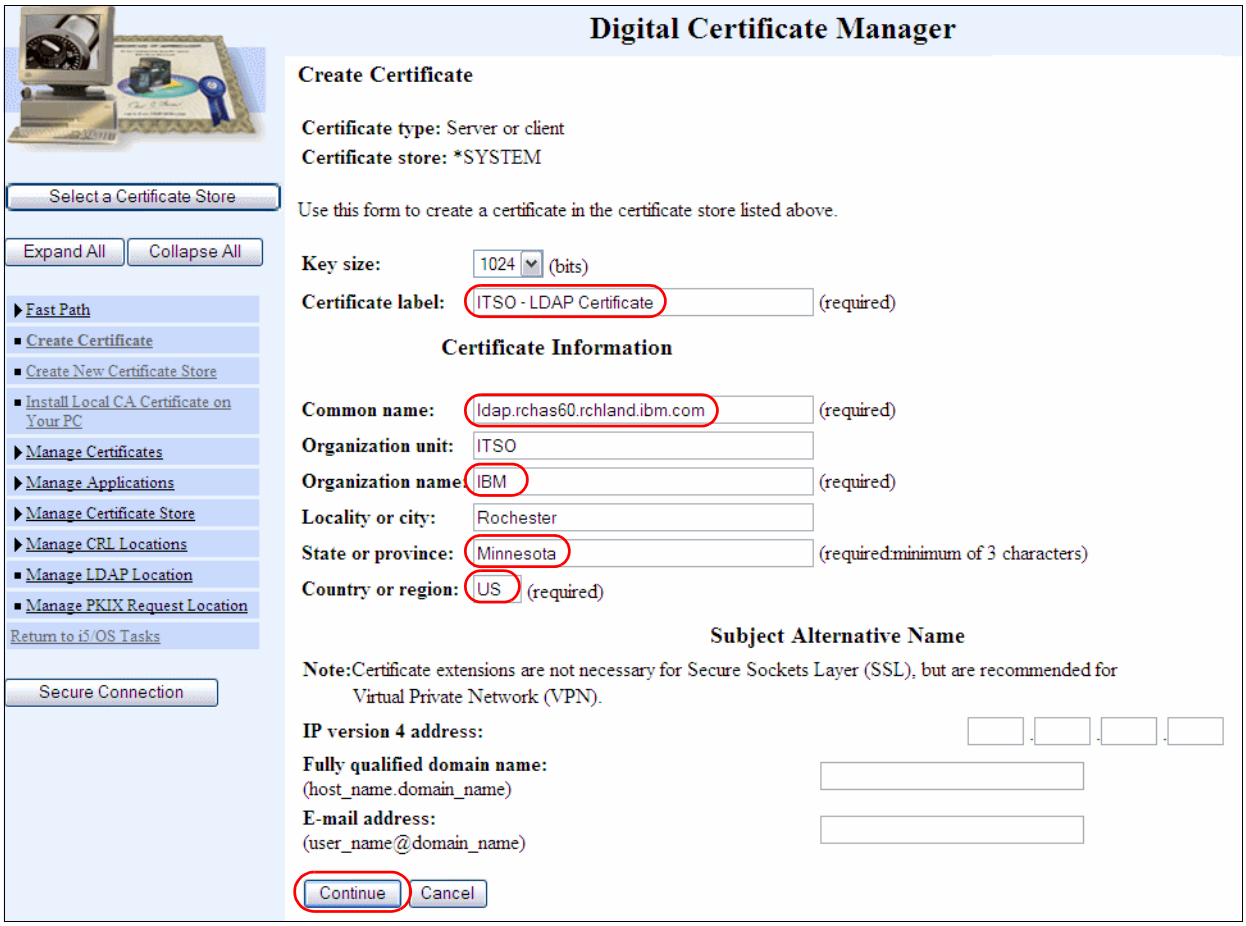


Figure 5-29 Entering the certificate information

9. The certificate is now created. You are also presented with a list of applications that you can configure to use this newly created certificate. Do *not* select any application in the list and click **Continue** (Figure 5-30).

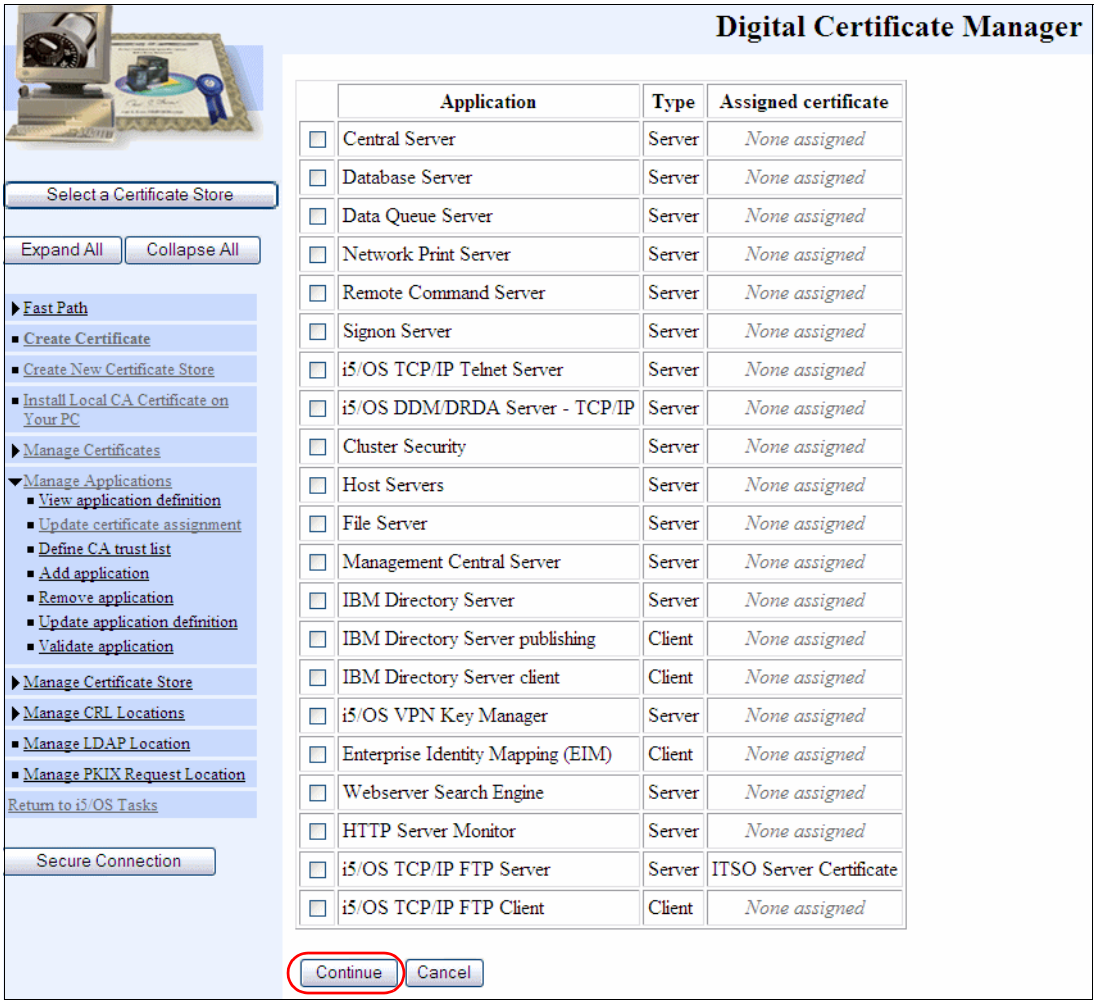

Digital Certificate Manager
Select a Certificate Store
Expand All
Collapse All
Fast Path
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
Manage Applications
View application definition
Update certificate assignment
Define CA trust list
Add application
Remove application
Update application definition
Validate application
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
Application
Type
Assigned certificate
Central Server Server None assigned
Database Server Server None assigned
Data Queue Server Server None assigned
Network Print Server Server None assigned
Remote Command Server Server None assigned
Signon Server Server None assigned
i5/OS TCP/IP Telnet Server Server None assigned
i5/OS DDM/DRDA Server - TCP/IP Server None assigned
Cluster Security Server None assigned
Host Servers Server None assigned
File Server Server None assigned
Management Central Server Server None assigned
IBM Directory Server Server None assigned
IBM Directory Server publishing Client None assigned
IBM Directory Server client Client None assigned
i5/OS VPN Key Manager Server None assigned
Enterprise Identity Mapping (EIM) Client None assigned
Webserver Search Engine Server None assigned
HTTP Server Monitor Server None assigned
i5/OS TCP/IP FTP Server Server ITSO Server Certificate
i5/OS TCP/IP FTP Client Client None assigned
Continue
Cancel

Figure 5-30 Do not select any applications at this stage

10. You are now shown the list of applications you have selected. This list is empty. Click **OK** (Figure 5-31).

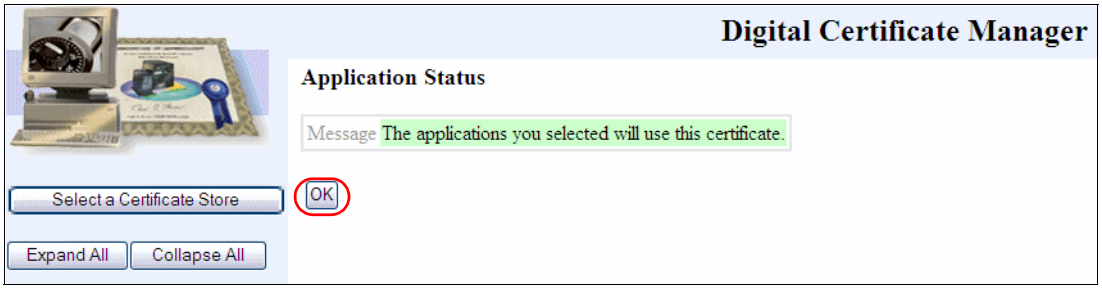


Figure 5-31 Application status - empty list

11. In the left navigation pane, expand **Manage Applications** and click **Update certificate assignment** (Figure 5-32).

Figure 5-32 Managing certificates

12. Select **Server** and click **Continue** (Figure 5-33).

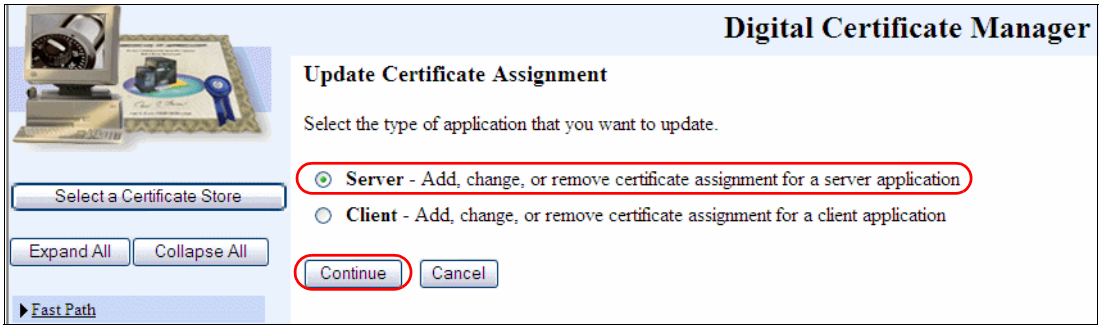

Digital Certificate Manager
Update Certificate Assignment
Select the type of application that you want to update.
Server - Add, change, or remove certificate assignment for a server application
Client - Add, change, or remove certificate assignment for a client application
Continue
Cancel
Select a Certificate Store
Expand All
Collapse All
Fast Path

Figure 5-33 Updating the server certificate assignment

13. Select **IBM Directory Server** and click **Update Certificate Assignment** (Figure 5-34).

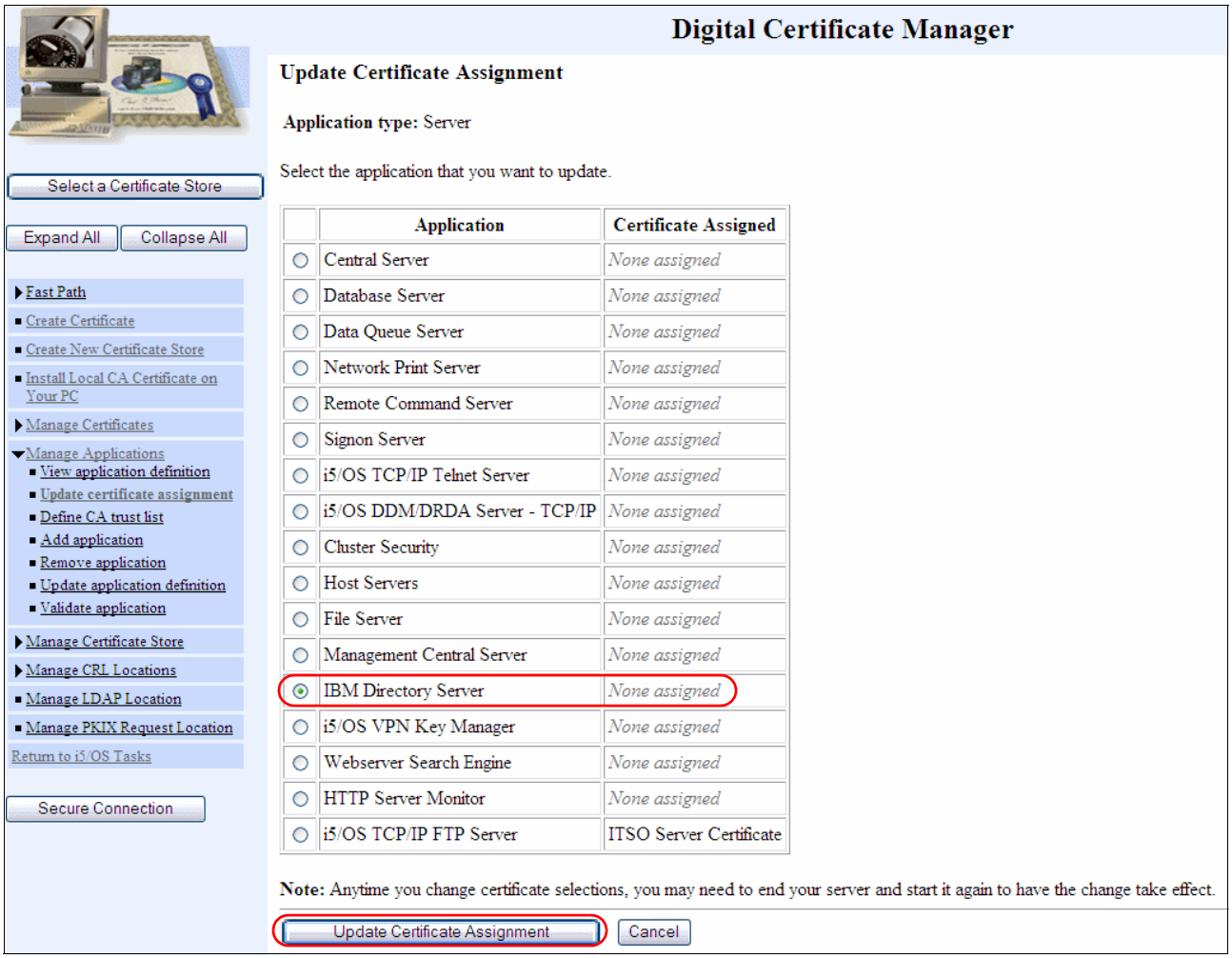


Figure 5-34 Selecting the server

14. A list of available certificates to assign to the IBM Directory Server is displayed. Select the certificate created for that purpose and click **Assign New Certificate** (Figure 5-35).

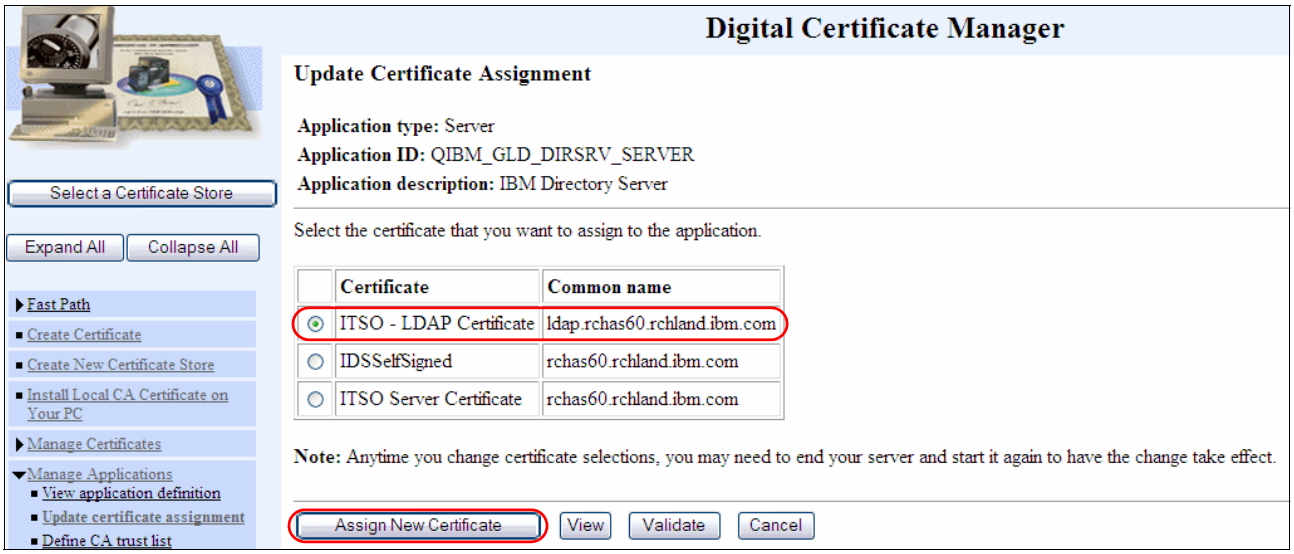


Figure 5-35 Assigning the new certificate to the IBM Directory Server

15. A confirmation message and summary of the certificate assignment is displayed (Figure 5-36).

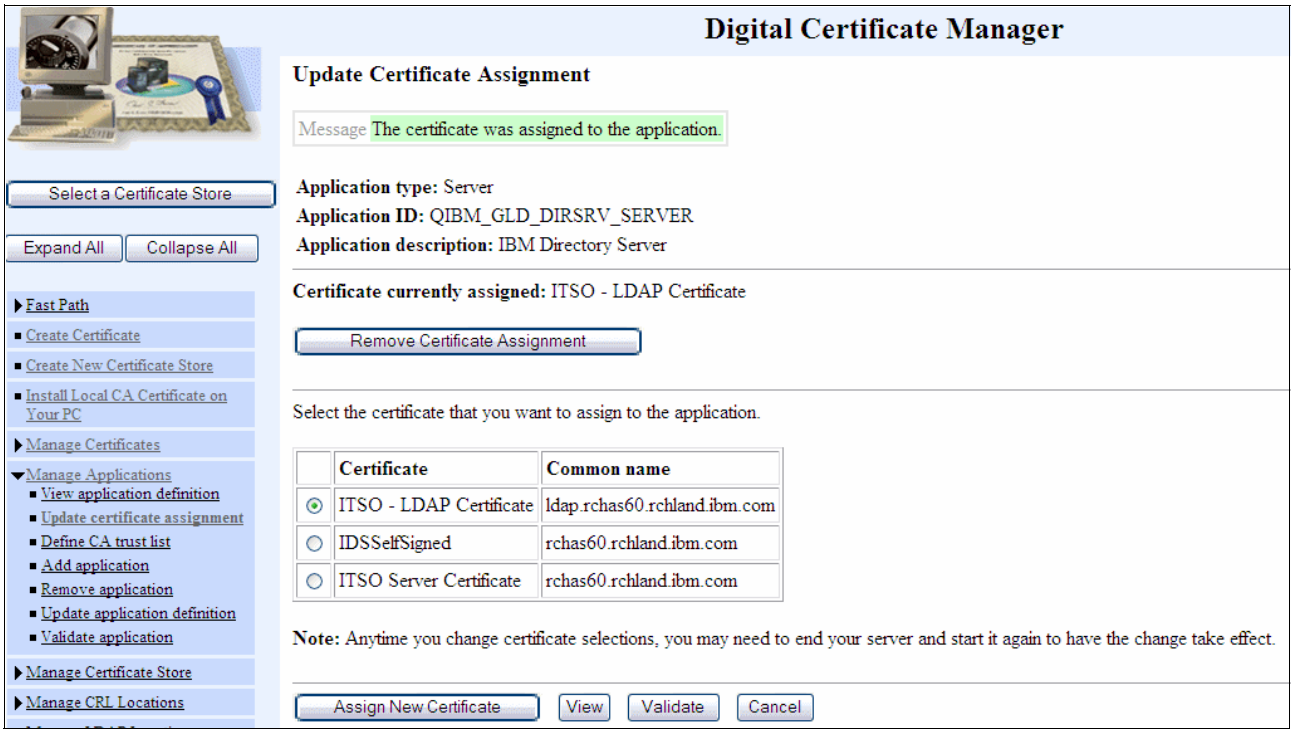


Figure 5-36 Certificate assignment summary

16. Restart the IBM Directory Server for the changes to become effective. You can use the following i5/OS CL commands to restart the IBM Directory Server:

```
ENDTCPSVR SERVER(*DIRSRV)
STRTCPSVR SERVER(*DIRSRV)
```

Enabling SSL connections for the IBM Directory Server

You now need to configure the IBM Directory Server so that it accepts secured connections. Perform the following steps:

1. From the iSeries Navigator, select ***your_system*** → **Network** → **Servers** → **TCP/IP**, right-click **IBM Directory Server** and select **Properties** (Figure 5-37).

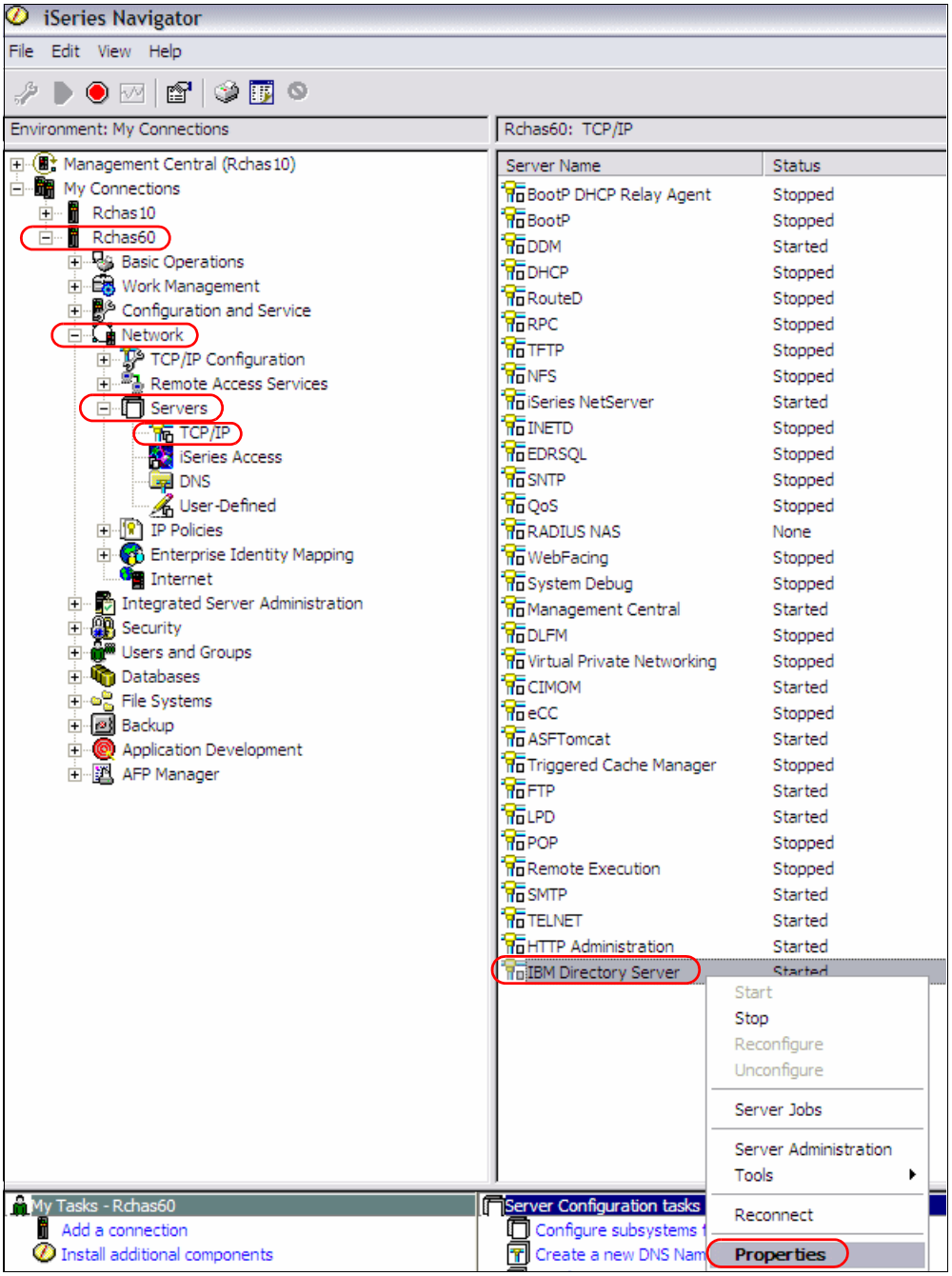


Figure 5-37 Configuring IBM Directory Server with iSeries Navigator

2. In the IBM Directory Server Properties window, select the **Network** tab and check **Secure** in the Connections to allow section (Figure 5-38). Also, note the secure port used by the LDAP server because you need this port for the next step. Click **OK**.

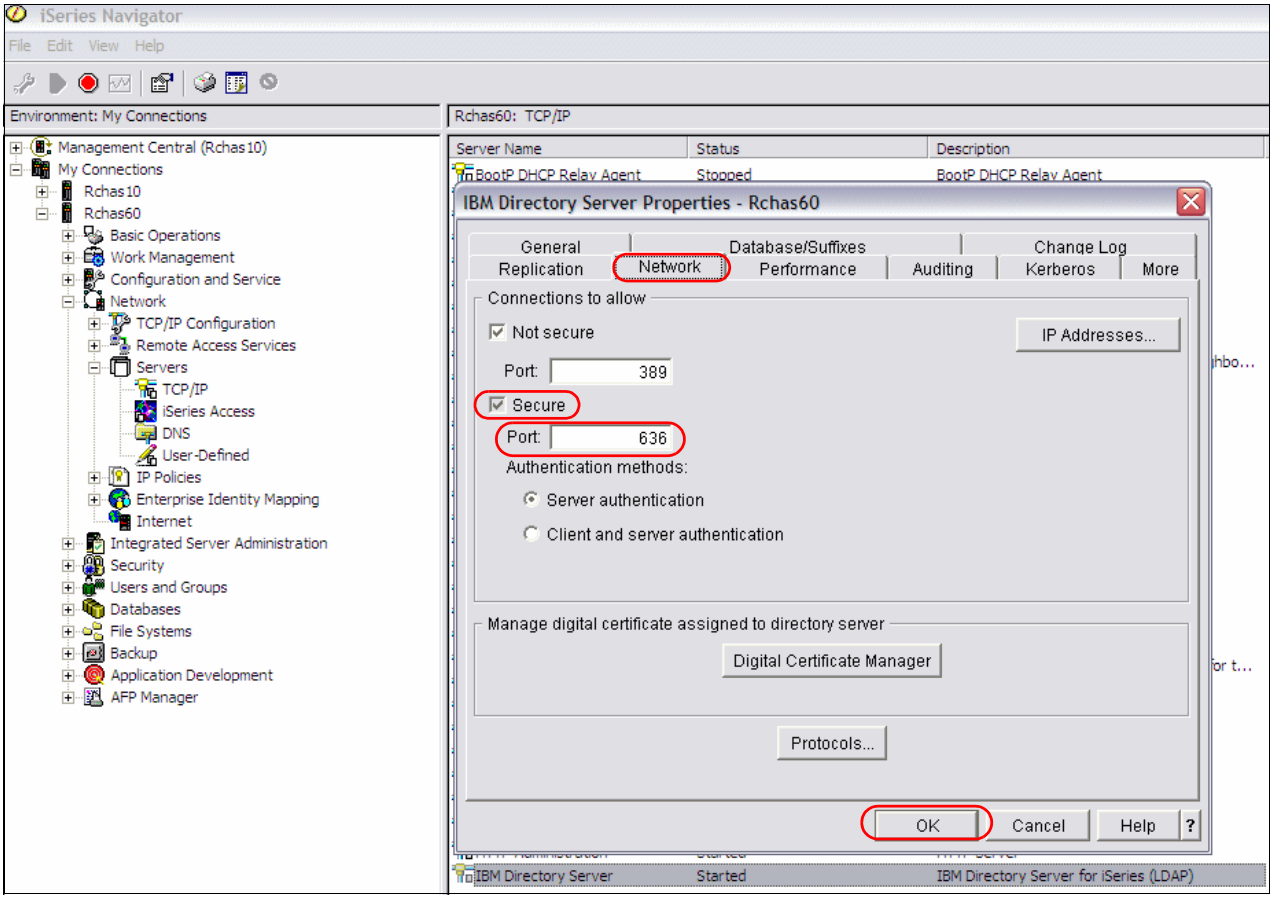


Figure 5-38 Enabling SSL for the LDAP server

3. Restart the IBM Directory Server for the change to become effective. From the iSeries Navigator, select ***your_system*** → **Network** → **Servers** → **TCP/IP**, right-click **IBM Directory Server** and select **Stop**, then select **Start** (Figure 5-39).

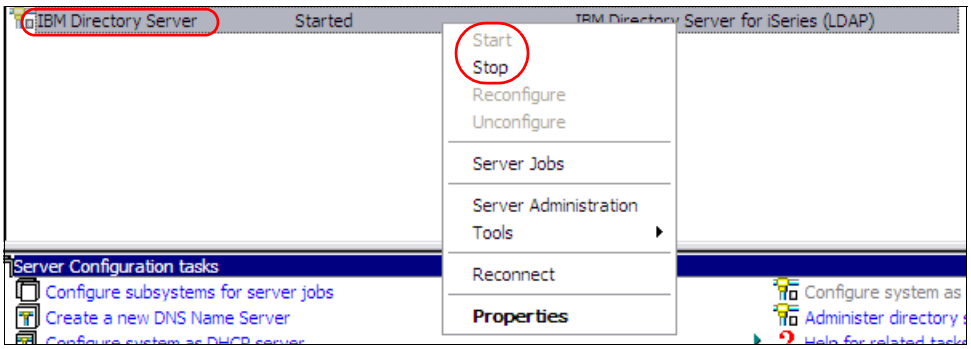


Figure 5-39 Stopping and starting IBM Directory Server

5.1.3 Enabling SSL for WebSphere Portal Express

You can configure WebSphere Portal Express to use a specifically named key store so that WebSphere Portal Express and WebSphere Application Server can share the same trust store in the SSL configuration.

Important: You need to perform the following first seven steps only if WebSphere Application Server has been configured to use LDAP as the user registry. If you configured your WebSphere Portal Express instance using the Create New WebSphere Portal wizard in the IBM Web Administration for i5/OS, then WebSphere Application Server is configured to use the WebSphere Member Manager database as the user registry. In that case, skip Steps 1 to 7 and begin with Step 8.

1. Stop WebSphere Portal Express and start WebSphere Application Server (server1).
2. Log in to the WebSphere Application Server administration console.
3. Navigate to the LDAP User Registry panel.
4. Check the **sslEnabled** box.
5. Set the LDAP port to the value that you noted while performing “Enabling SSL for the LDAP server” on page 170.
6. Save the changes to the master configuration.
7. Stop WebSphere Application Server (server1).
8. Edit the file wmm.xml located in the directory of /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_instance*/PortalServer/wmm.
9. Navigate to the xml tag beginning with <*ldapRepository name*=“wmmLDAP”.
10. Set the attribute ldapPort to the value that you noted while performing “Enabling SSL for the LDAP server” on page 170. See Figure 5-40 on page 182.
11. Set the attribute sslEnabled value to `true` (Figure 5-40 on page 182).

12. Set the attribute sslTrustStore to the value `/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/portal_instance/etc/DummyServerTrustFile.jks` (Figure 5-40).

```
 <ldapRepository name="wmmLDAP"
                 UUID="LDAP1"

adapterClassName="com.ibm.ws.wmm.ldap.ibmdir.IBMDirectoryAdapterImpl"
                 supportDynamicAttributes="false"
                 configurationFile="wmmLDAPServerAttributes.xml"
                 wmmGenerateExtId="false"
                 supportGetPersonByAccountName="true"
                 profileRepositoryForGroups="LDAP1"
                 supportTransactions="false"
                 adminId="cn=administrator"
                 adminPassword="KbdgwOqBnh5aSDxgmrHpOg=="
                 ldapHost="rchas60.rchland.ibm.com"
                 ldapPort="636"
                 ldapTimeOut="6000"
                 ldapAuthentication="SIMPLE"
                 ldapType="0"
                 sslEnabled="true"

sslTrustStore="/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WPX6PRF/etc/
DummyServerTrustFile.jks"
                 dirContextsMaxSize="20"
                 dirContextsMinSize="5"
                 dirContextTimeToLive="-1"
                 cacheGroups="false"
                 groupsCacheTimeOut="600"
                 cacheAttributes="true"
                 attributesCacheSize="2000"
                 attributesCacheTimeOut="600"
                 cacheNames="true"
                 namesCacheSize="2000"
                 namesCacheTimeOut="600"
                 ignoreReadOnlyUpdate="true">
```

Figure 5-40 Editing the wmm.xml file to enable SSL

13. Save the file.
14. Stop and restart WebSphere Portal Express.
15. To validate the SSL configuration, check that you can log in to WebSphere Portal Express.
16. To check that LDAP and WebSphere Portal Express are using SSL to communicate, use the i5/OS CL command of Work with TCP/IP Network Status (NETSTAT). On the Work with TCP/IP Network Status, type option 3 (Work with TCP/IP connection status) and press Enter. On the Work with TCP/IP connection status, press PF14 (Display port numbers) to display port numbers. Page down until you find your secured LDAP port in the Remote Port column. Check that the connection is established (Figure 5-41 on page 183).

```
                  Work with TCP/IP Connection Status
                                                                 System:   RCHAS60
Type options, press Enter.
  3=Enable debug   4=End   5=Display details   6=Disable debug
  8=Display jobs

     Remote           Remote  Local
Opt  Address           Port    Port  Idle Time  State
     *                    *   8020  000:07:24  Listen
     *                    *   5988  098:05:33  Listen
     *                    *  20759  098:05:51  Listen
     *                    *  30543  098:05:52  Listen
     9.5.92.19        36565     23  000:01:14  Established
     9.5.92.48        41662     23  000:02:15  Established
     9.5.92.95          636  16246  000:43:35  Established
     9.5.92.95          636  16823  000:43:35  Established
     9.5.92.95          636  20847  000:43:26  Established
     9.5.92.95          636  21039  000:43:35  Established
     9.5.92.95          636  55830  000:07:14  Established
     9.5.92.95        10238  23286  000:06:41  Close-wait
                                                                       More...
F3=Exit   F5=Refresh   F9=Command line   F11=Display byte counts   F12=Cancel
F15=Subset   F20=Work with IPv6 connections   F24=More keys
```

Figure 5-41 Checking connection port and status

5.2 SSL between WebSphere Portal Express and Web browser

This section describes the process to implement SSL between WebSphere Portal Express and the client Web browser. If the content served by your portal is not critical or confidential, you might want to only secure the login process. If the content is critical or confidential, then you need to secure every single page that the portal will serve.

Setting up SSL between WebSphere Portal Express and the client Web browser implies the following steps (the concept remains the same if you enable SSL for login only or for all pages):

- 5.2.1, “Enabling the HTTP server for SSL” on page 183
- 5.2.2, “Enabling WebSphere Application Server for SSL” on page 198
- 5.2.3, “Enabling WebSphere Portal Express for SSL: login only” on page 217 or 5.2.4, “Enabling WebSphere Portal Express for SSL: All pages” on page 227

Enabling SSL means that you must configure the Web server to accept inbound SSL traffic. Then you configure the WebSphere Application Server plugin for the Web server to forward traffic to WebSphere Application Server and WebSphere Portal Express. This involves configuring the virtual host information. Finally, you must set up WebSphere Portal Express to generate self-referencing URLs using SSL as the transport.

5.2.1 Enabling the HTTP server for SSL

To enable SSL for the HTTP server, you need to enable the HTTP server to accept connections over SSL and then create and associate a key certificate to the HTTP server.

Important: For a production environment, you might prefer to get a certificate from a third-party CA (for example, Equifax or Verisign) instead of creating a self-signed certificate.

Enabling SSL for the HTTP Server

To enable SSL communication for the HTTP server, perform the following steps:

1. Create a virtual host:
   a. Open a Web browser and log in to the IBM Web Administration for i5/OS interface.
   b. Select the **Manage** tab, then the **HTTP Servers** tab, and select your HTTP server from the drop-down list (Figure 5-42).

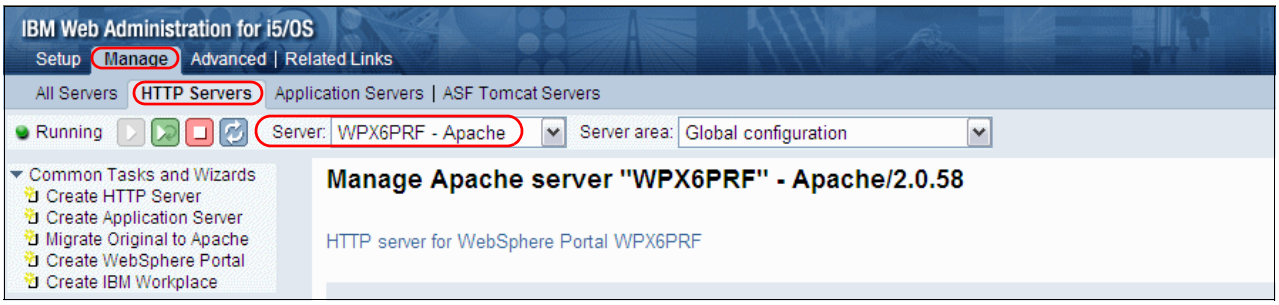


Figure 5-42 Selecting your HTTP server

   c. In the left navigation pane, expand **Server Properties** and select **Virtual Hosts** (Figure 5-43).

IBM Web Administration for i5/OS
Setup
Manage
Advanced | Related Links
WebSphere
IBM
All Servers
HTTP Servers
Application Servers | ASF Tomcat Servers
Running
Server: WPX6PRF - Apache
Server area: Global configuration
Common Tasks and Wizards
Create HTTP Server
Create Application Server
Migrate Original to Apache
Create WebSphere Portal
Create IBM Workplace
HTTP Tasks and Wizards
Add a Directory to the Web
LDAP Configuration
Servlet and JSP Enablement
Server Properties
General Server Configuration
Container Management
Virtual Hosts
URL Mapping
Manage Apache server "WPX6PRF" - Apache/2.0.58
HTTP server for WebSphere Portal WPX6PRF
Welcome to the IBM Web Administration for i5/OS manage forms for HTTP Server (powered by Apache).
Using these forms, you can set up and manage your HTTP Server (powered by Apache) quickly and easily.
With IBM HTTP Server for i5/OS, you have everything you need to establish a Web presence and get started
on the road to working the Web for business.
To get started, use the Create New HTTP Server wizard under Common Tasks and Wizards. Follow the wizard,
step by step, to quickly create a working HTTP Server (powered by Apache).
Once the wizard has been successfully completed, you will have an HTTP Server that is usable for internal or
external business needs.

Figure 5-43 Virtual hosts management

d. Select the **Name-based** tab and click **Add** (Figure 5-44).

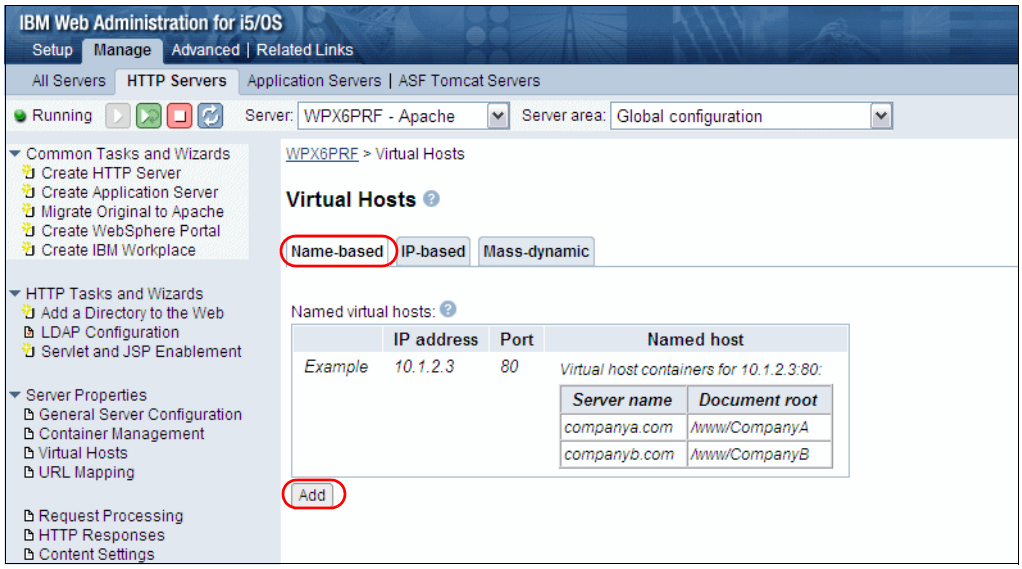


Figure 5-44 Adding a virtual host

e. Select the IP address on which the virtual host will listen from the drop-down list (Figure 5-45).

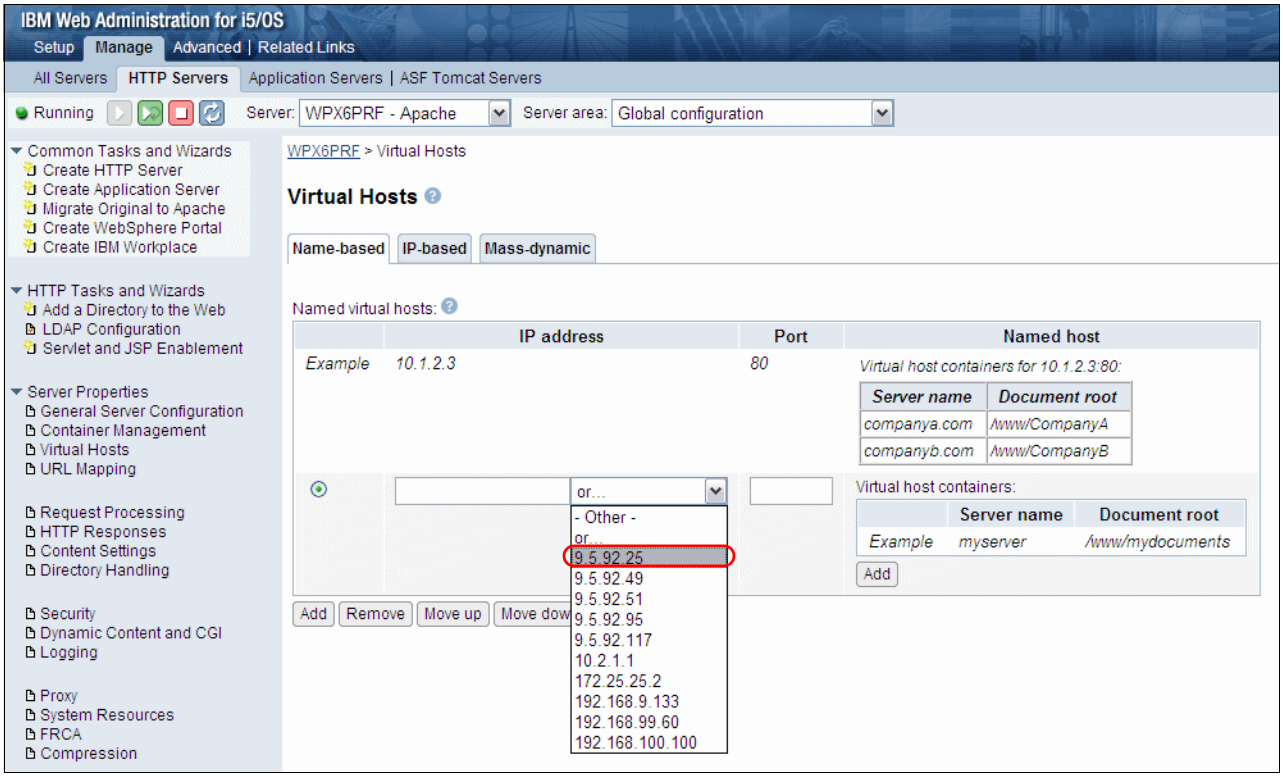


Figure 5-45 Selecting the IP address of the virtual host

f. Enter the secure port for the virtual host and click **Add** (Figure 5-46).

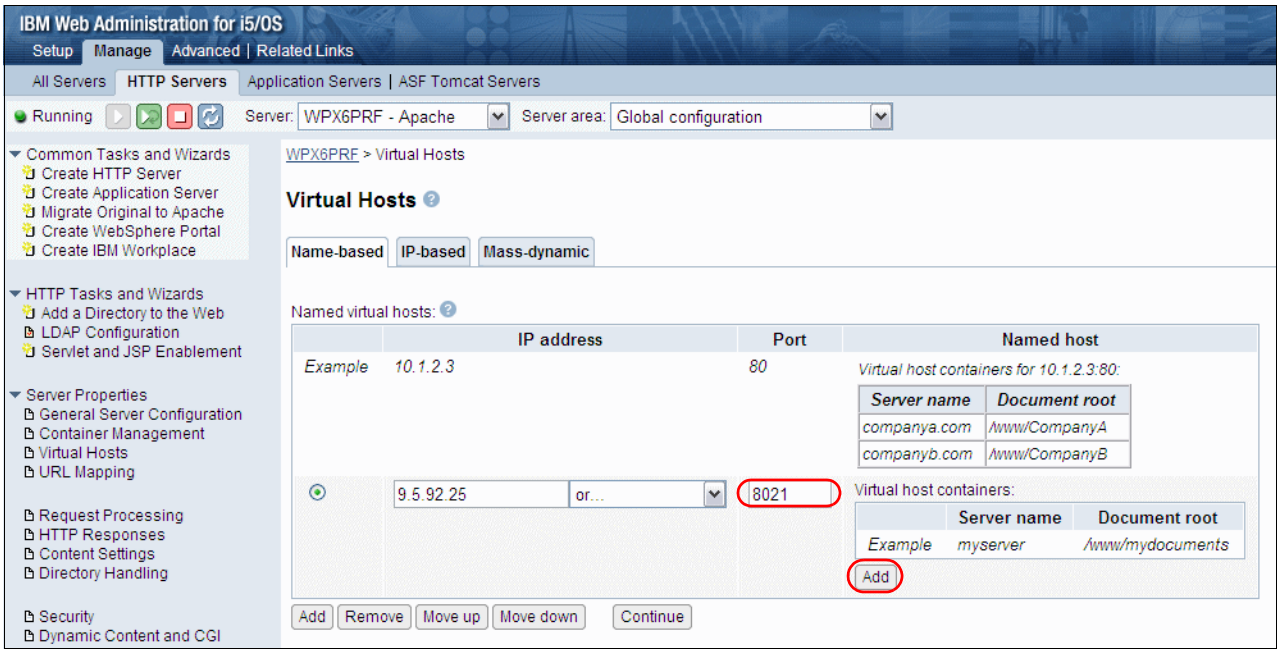


Figure 5-46 Setting the virtual host port

g. Enter the HTTP server name and click **Continue** (Figure 5-47).

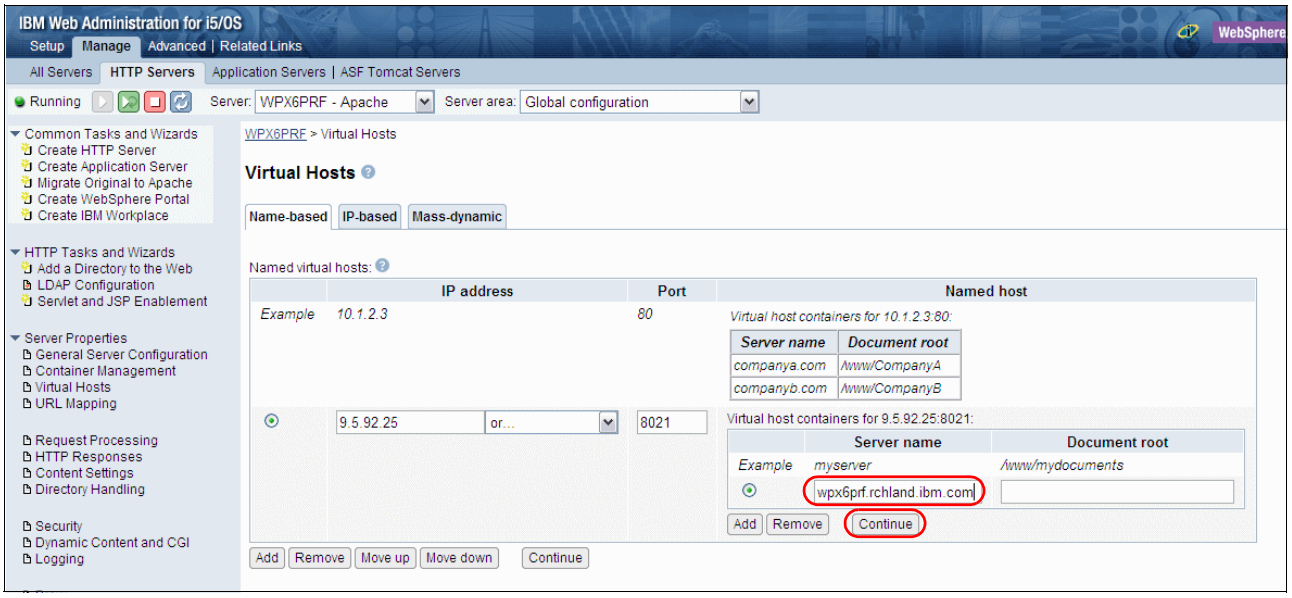


Figure 5-47 Setting the HTTP server name

h. Click **Continue** to create the virtual host (Figure 5-48). Then click **OK** to confirm the settings.

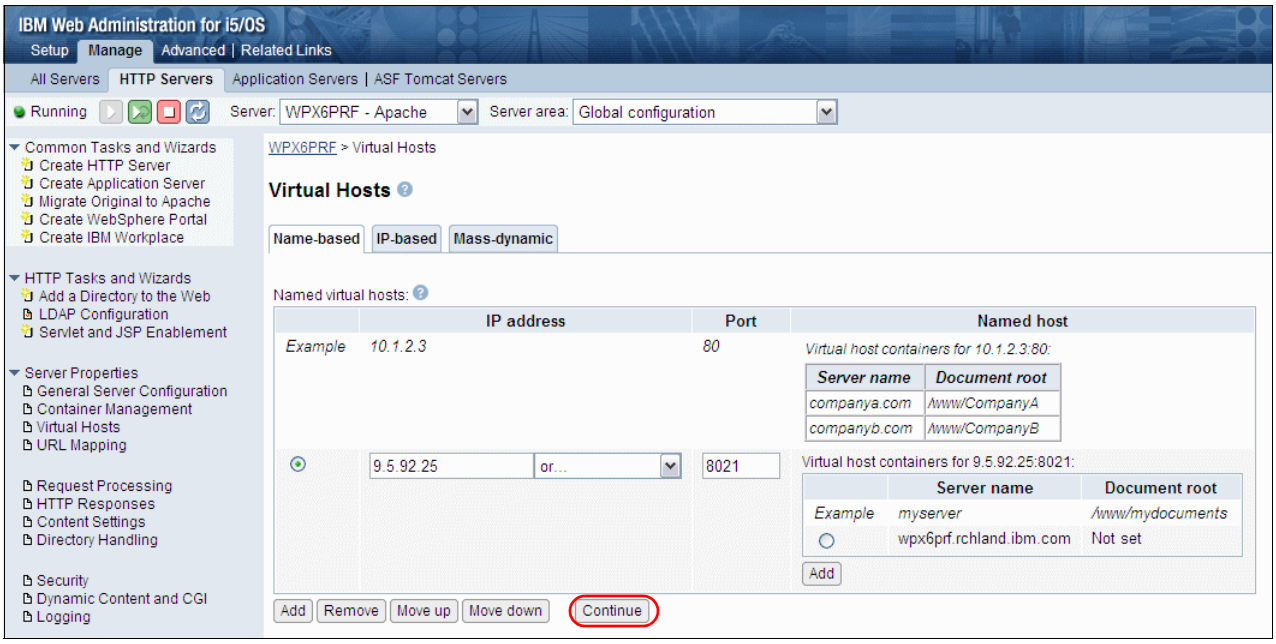


Figure 5-48 Creating the virtual host

i. Expand **Server Properties** and select **General Server Configuration**. Then select the **General Settings** tab and click **Add** (Figure 5-49).

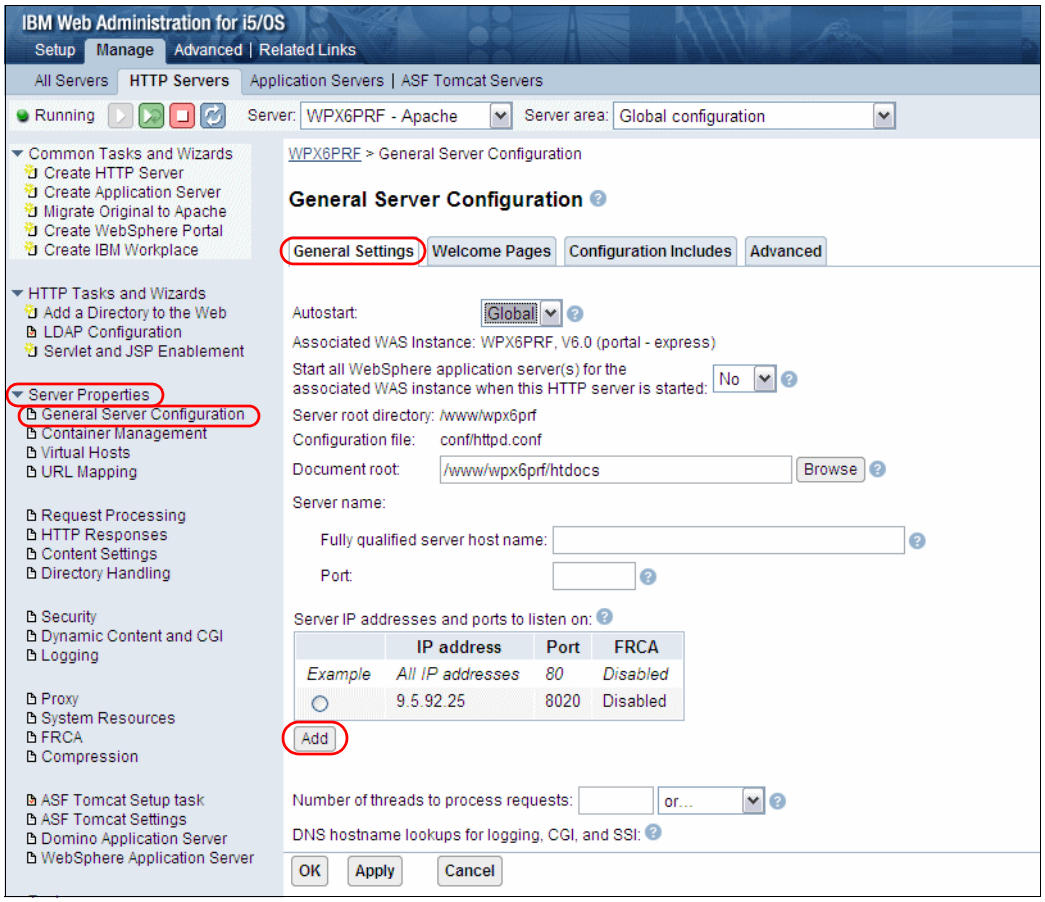


Figure 5-49 Adding a listen directive for the virtual host

j. Select the virtual host IP address from the drop-down list and then add the port on which it is listening. Click **Continue** (Figure 5-50). Click **OK** to confirm the settings.

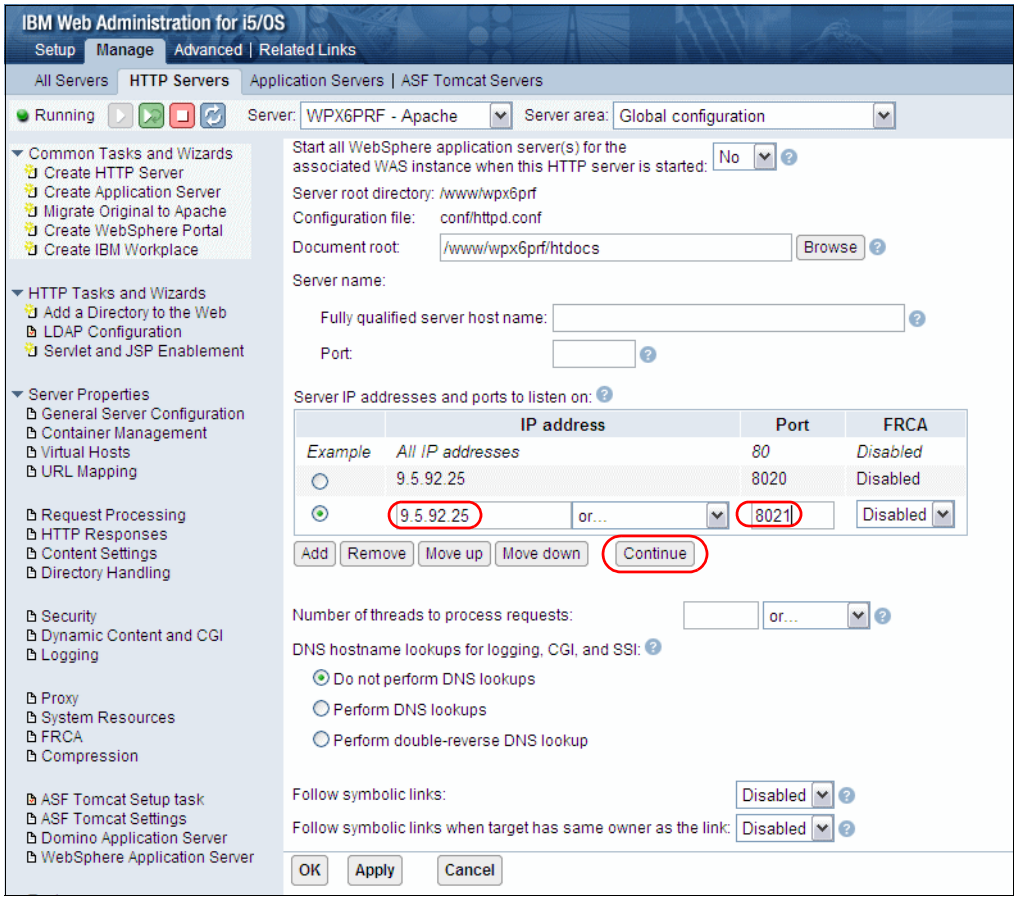


Figure 5-50 Setting the listen directive for the virtual host

2. Enable the virtual host for SSL communications:

   a. Select the virtual host in the **Server area** drop-down list (Figure 5-51).

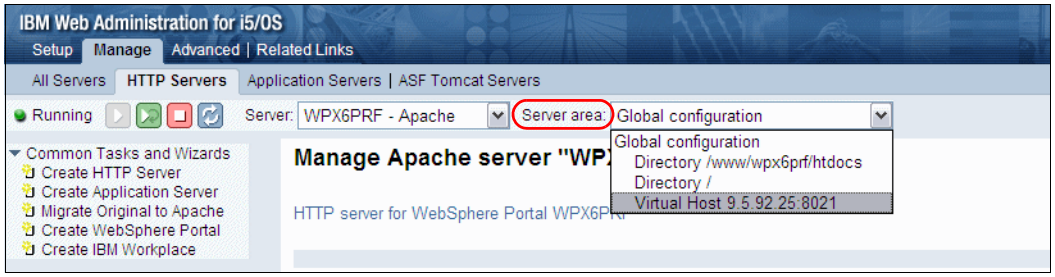


Figure 5-51 Managing the virtual host

b. Expand **Server Properties** and select **Security**. Select the **SSL with Certificate Authentication** tab. In the **SSL** drop-down list, select **Enabled** (Figure 5-52).

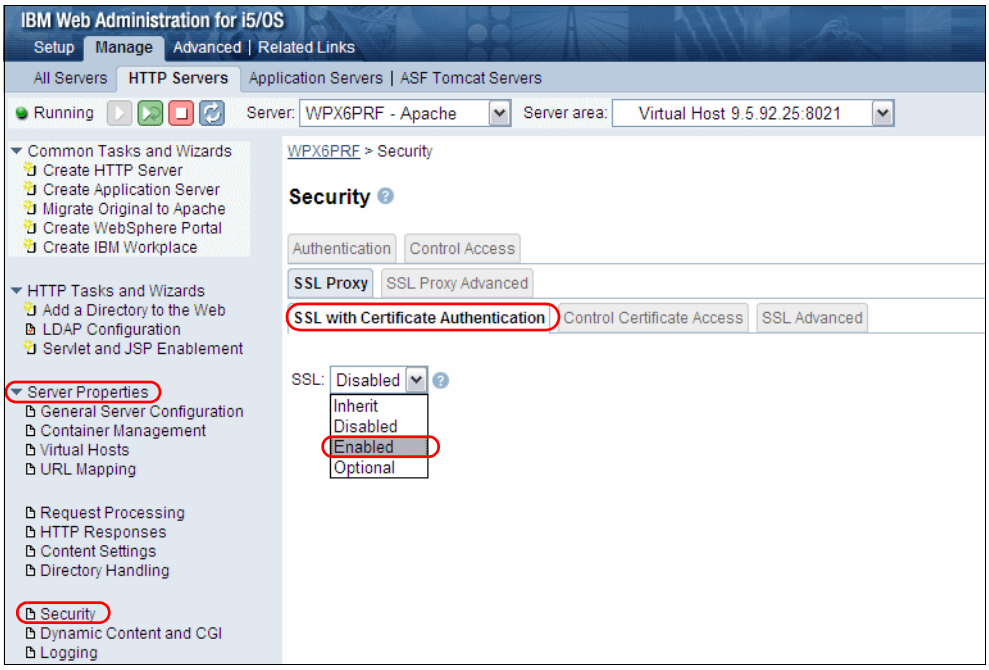


Figure 5-52 Enabling SSL for the virtual host

c. In the **Server certificate application name** drop-down list, select the HTTP server certificate application name. In our example, this is `QIBM_HTTP_SERVER_WPX6PRF` as shown in Figure 5-53. Click **Apply**.

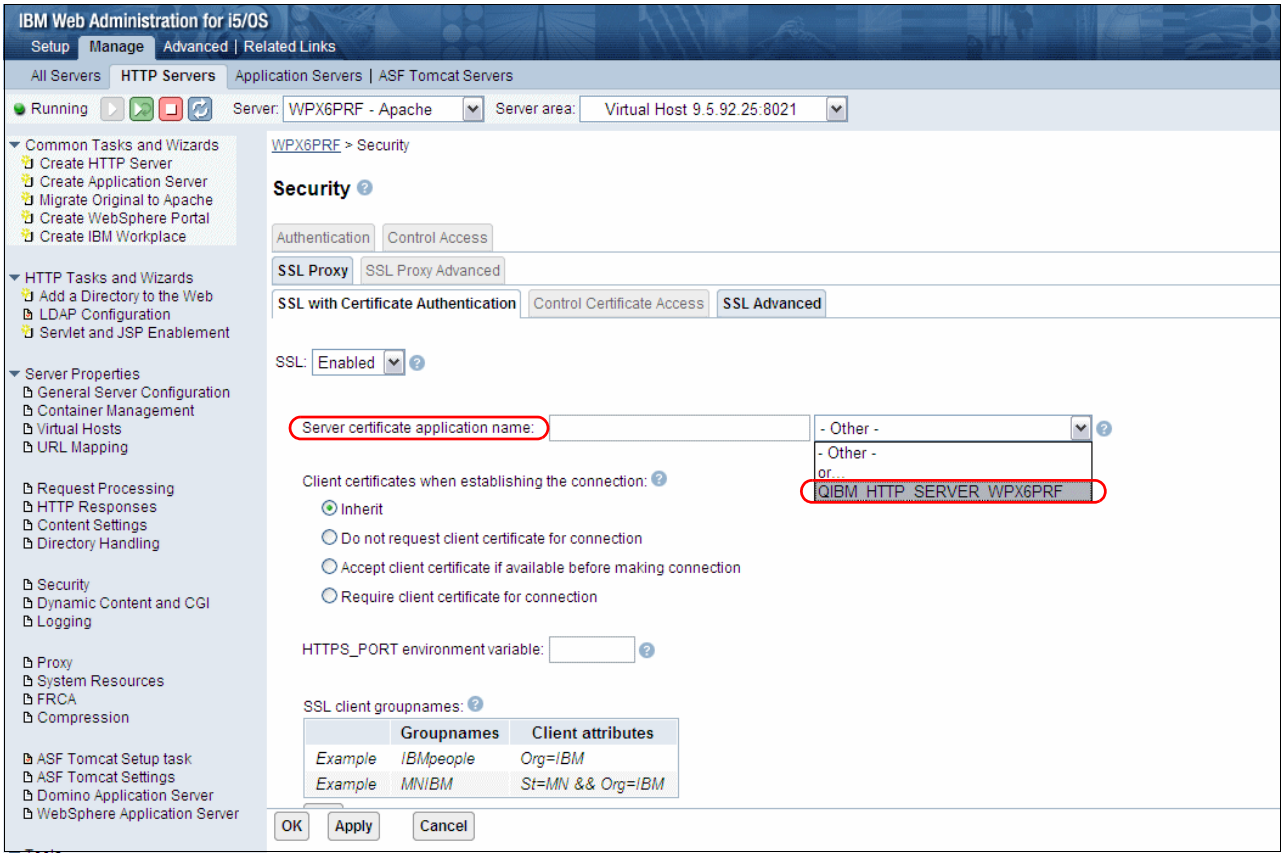


Figure 5-53 Selecting the server certificate application name

3. Check that the configuration file of the HTTP server contains the HTTP directives for the virtual host that you just created:

   a. Expand **Tools** and click **Display Configuration File** (Figure 5-54).

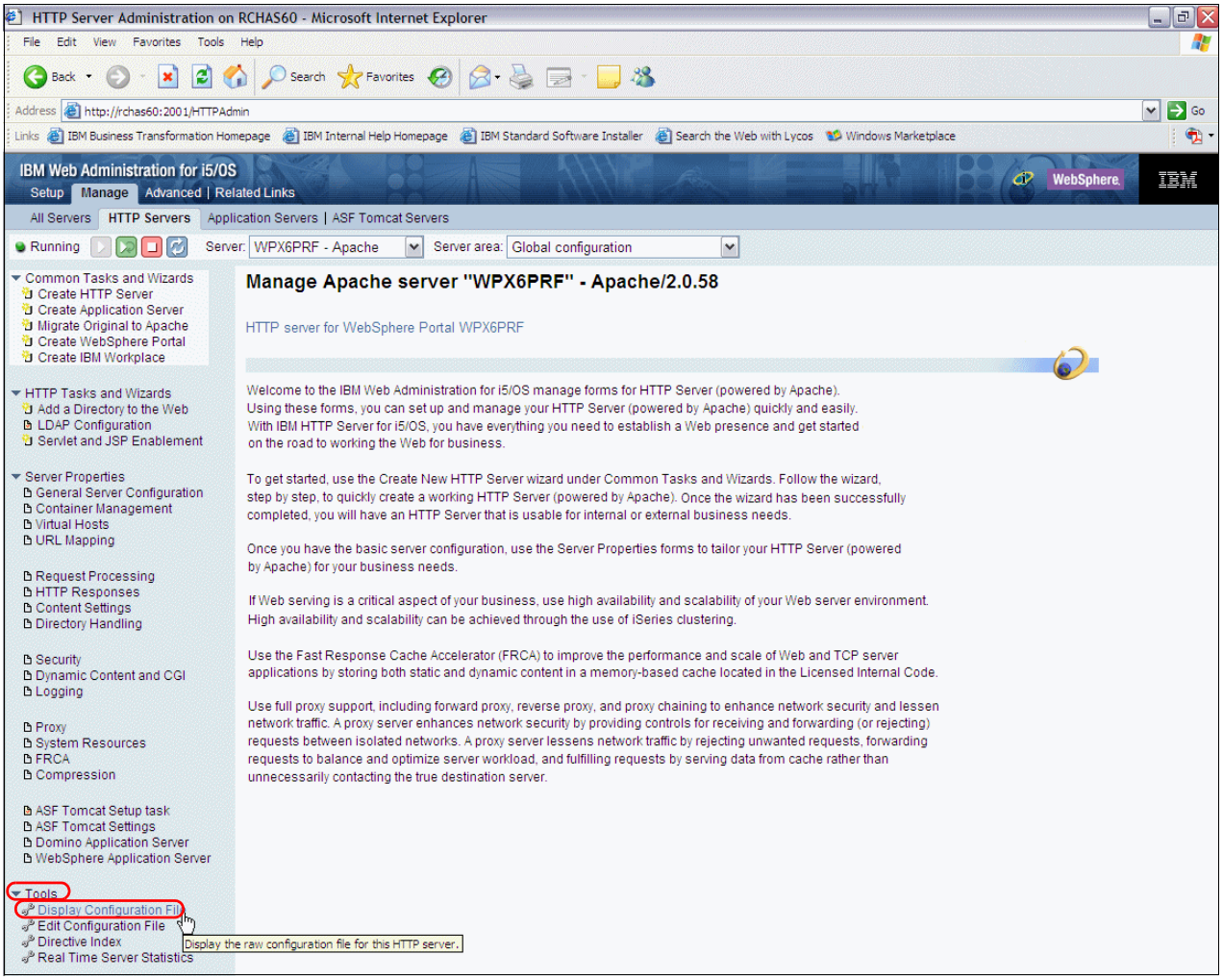

HTTP Server Administration on RCHAS60 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://rchas60:2001/HTTPAdmin
Links IBM Business Transformation Homepage IBM Internal Help Homepage IBM Standard Software Installer Search the Web with Lycos Windows Marketplace
IBM Web Administration for i5/OS
Setup Manage Advanced | Related Links
WebSphere
IBM
All Servers HTTP Servers Application Servers | ASF Tomcat Servers
Running
Server: WPX6PRF - Apache
Server area: Global configuration
Common Tasks and Wizards
Create HTTP Server
Create Application Server
Migrate Original to Apache
Create WebSphere Portal
Create IBM Workplace
HTTP Tasks and Wizards
Add a Directory to the Web
LDAP Configuration
Servlet and JSP Enablement
Server Properties
General Server Configuration
Container Management
Virtual Hosts
URL Mapping
Request Processing
HTTP Responses
Content Settings
Directory Handling
Security
Dynamic Content and CGI
Logging
Proxy
System Resources
FRCA
Compression
ASF Tomcat Setup task
ASF Tomcat Settings
Domino Application Server
WebSphere Application Server
Tools
Display Configuration File
Edit Configuration File
Directive Index
Real Time Server Statistics
Display the raw configuration file for this HTTP server.
Manage Apache server "WPX6PRF" - Apache/2.0.58
HTTP server for WebSphere Portal WPX6PRF
Welcome to the IBM Web Administration for i5/OS manage forms for HTTP Server (powered by Apache).
Using these forms, you can set up and manage your HTTP Server (powered by Apache) quickly and easily.
With IBM HTTP Server for i5/OS, you have everything you need to establish a Web presence and get started on the road to working the Web for business.
To get started, use the Create New HTTP Server wizard under Common Tasks and Wizards. Follow the wizard, step by step, to quickly create a working HTTP Server (powered by Apache). Once the wizard has been successfully completed, you will have an HTTP Server that is usable for internal or external business needs.
Once you have the basic server configuration, use the Server Properties forms to tailor your HTTP Server (powered by Apache) for your business needs.
If Web serving is a critical aspect of your business, use high availability and scalability of your Web server environment. High availability and scalability can be achieved through the use of iSeries clustering.
Use the Fast Response Cache Accelerator (FRCA) to improve the performance and scale of Web and TCP server applications by storing both static and dynamic content in a memory-based cache located in the Licensed Internal Code.
Use full proxy support, including forward proxy, reverse proxy, and proxy chaining to enhance network security and lessen network traffic. A proxy server enhances network security by providing controls for receiving and forwarding (or rejecting) requests between isolated networks. A proxy server lessens network traffic by rejecting unwanted requests, forwarding requests to balance and optimize server workload, and fulfilling requests by serving data from cache rather than unnecessarily contacting the true destination server.

Figure 5-54 Displaying the HTTP server configuration file

b. The configuration file of your HTTP server is similar to the one displayed in Figure 5-55.

```
LoadModule ibm_ssl_module /QSYS.LIB/QHTTPSVR.LIB/QZSRVSSL.SRVPGM
WebSpherePluginConfig
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WPX6PRF/config/cells/RCHAS6
0_WPX6PRF/nodes/IHS_RCHAS60_WPX6PRF_node/servers/IHS_RCHAS60_WPX6PRF/plugin-cfg
.xml
LoadModule was_ap20_module /QSYS.LIB/QWAS6.LIB/QSVTAP20.SRVPGM
DocumentRoot /www/wpx6prf/htdocs
ServerRoot /www/wpx6prf
Options -ExecCGI -FollowSymLinks -SymLinksIfOwnerMatch -Includes
-IncludesNoExec -Indexes -MultiViews
Listen 9.5.92.25:8020
Listen 9.5.92.25:8021
AccessFileName .htaccess
NameVirtualHost 9.5.92.25:8021
LogFormat "%{Cookie}n \"%r\" %t" cookie
LogFormat "%{User-agent}i" agent
LogFormat "%{Referer}i -> %U" referer
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
CustomLog logs/access_log combined
SetEnvIf "User-Agent" "JDK/1\.0" force-response-1.0
SetEnvIf "User-Agent" "Java/1\.0" force-response-1.0
SetEnvIf "User-Agent" "RealPlayer 4\.0" force-response-1.0
SetEnvIf "User-Agent" "MSIE 4\.0b2;" nokeepalive
SetEnvIf "User-Agent" "MSIE 4\.0b2;" force-response-1.0
SetEnvIf "User-Agent" "Mozilla/2" nokeepalive
DirectoryIndex index.html
<Directory /www/wpx6prf/htdocs>
   Order Allow,Deny
   Allow From all
</Directory>
<Directory />
   Order Deny,Allow
   Deny From all
</Directory>
<VirtualHost 9.5.92.25:8021>
   ServerName wpx6prf.rchland.ibm.com
   SSLEngine On
   SSLAppName QIBM_HTTP_SERVER_WPX6PRF
</VirtualHost>
# HTTP server (powered by Apache) configuration
```

Figure 5-55 HTTP server configuration file

Creating the key certificate for the HTTP server

To assign the key certificate to the HTTP server, perform the following steps:

1. Create the key certificate for the HTTP server, see Steps 1 to 10 of “Creating the key certificate for IBM Directory Server” on page 171.
2. Log in to the Digital Certificate Manager (see “Creating a certificate store” on page 156 to access the Digital Certificate Manager).

3. In the left navigation pane of the Digital Certificate Manger window, expand **Manage Applications** and click **Update certificate assignment** (Figure 5-56).

Figure 5-56 Updating certificate assignment

4. On the Update Certificate Assignment window, select **Server** and click **Continue** (Figure 5-57).

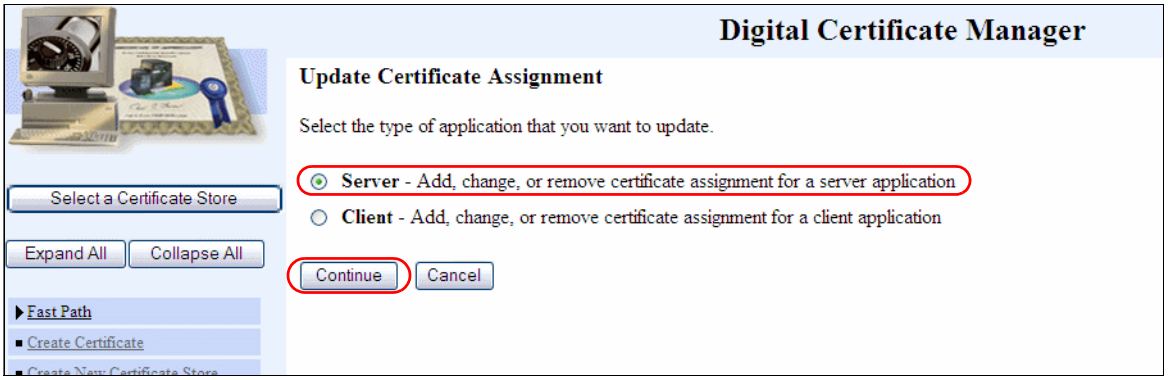

Digital Certificate Manager
Update Certificate Assignment
Select the type of application that you want to update.
Server - Add, change, or remove certificate assignment for a server application
Client - Add, change, or remove certificate assignment for a client application
Continue
Cancel
Select a Certificate Store
Expand All
Collapse All
Fast Path
Create Certificate

Figure 5-57 Updating the server certificate assignment

5. Select the HTTP Server application from the list. The HTTP Server application name has the pattern of QIBM_HTTP_SERVER_*httpServerName*. In our example, it is `QIBM_HTTP_SERVER_WPX6PRF`. Click **Update Certificate Assignment** (Figure 5-58).

Figure 5-58 Selecting the HTTP server application

6. Select the certificate you created for the HTTP server and click **Assign New Certificate** (Figure 5-59).

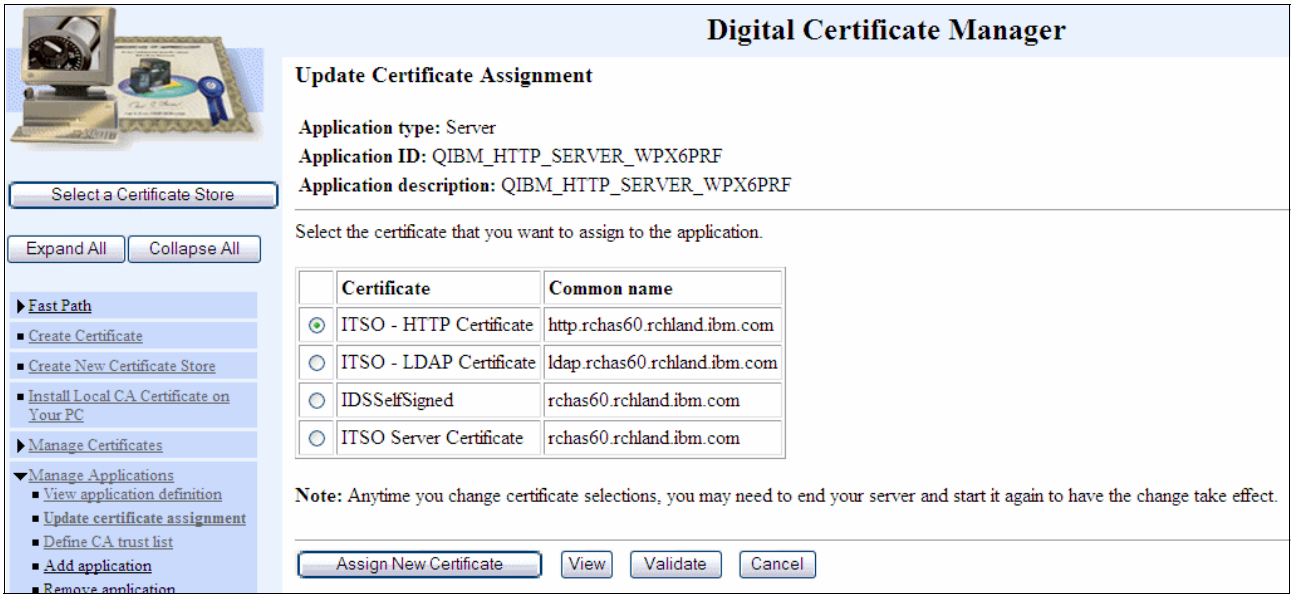


Figure 5-59 Assigning the certificate to the HTTP server

7. You are shown a confirmation message and a summary of the certificate assignment (Figure 5-60).

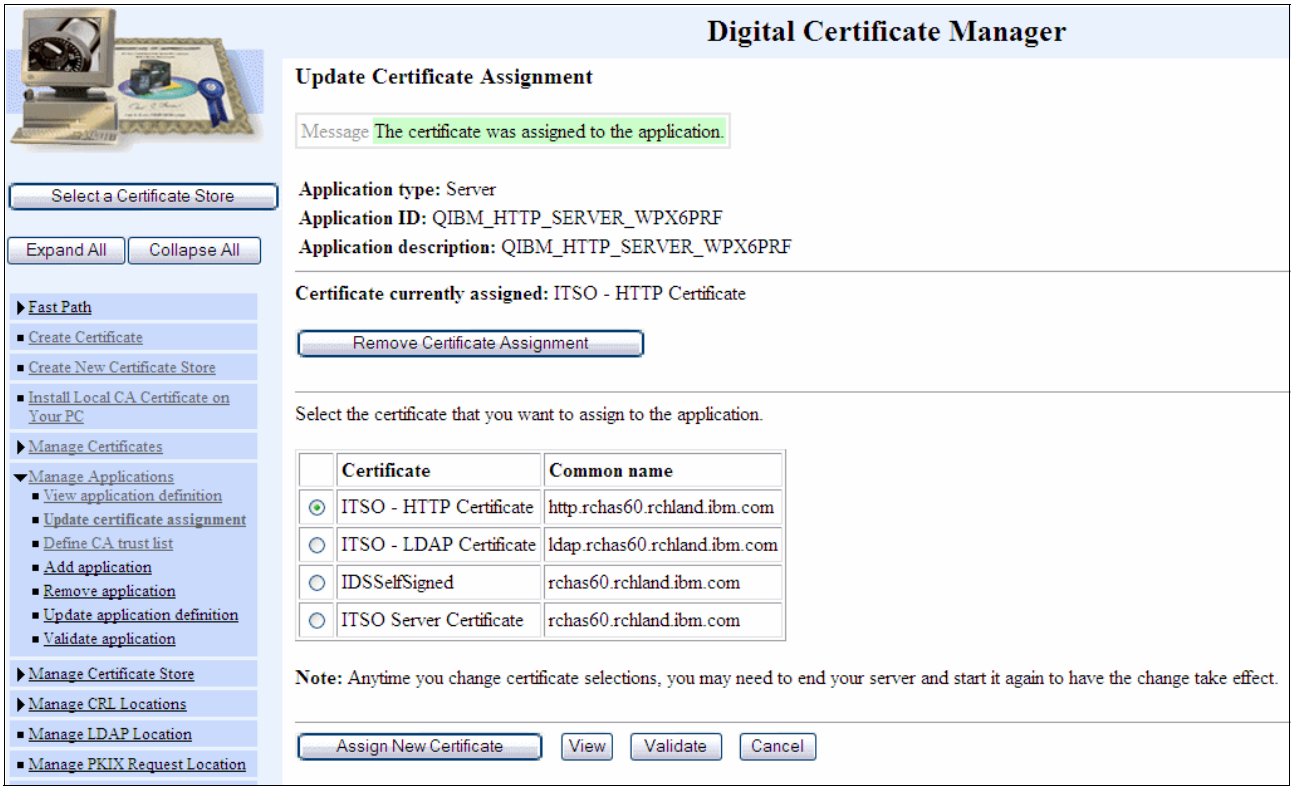


Figure 5-60 Certificate assignment summary

8. You can now close the Web browser. Restart the HTTP server for the changes to become effective. Use the following i5/OS CL commands to restart the HTTP Server:

   ```
   ENDTCPSVR SERVER(*HTTP) HTTPSVR(httpServerName)
   STRTCPSVR SERVER(*HTTP) HTTPSVR(httpServerName)
   ```

   In our example, httpServerName has the value `WPX6PRF`.

Checking the HTTP server configuration

Perform the following steps to check the HTTP server configuration:

1. Open a Web browser and enter the nonsecure URL of the HTTP server. In our example, this is `http://wpx6prf.rchland.ibm.com:8020`. You see the default home page of the HTTP server as shown in Figure 5-61.

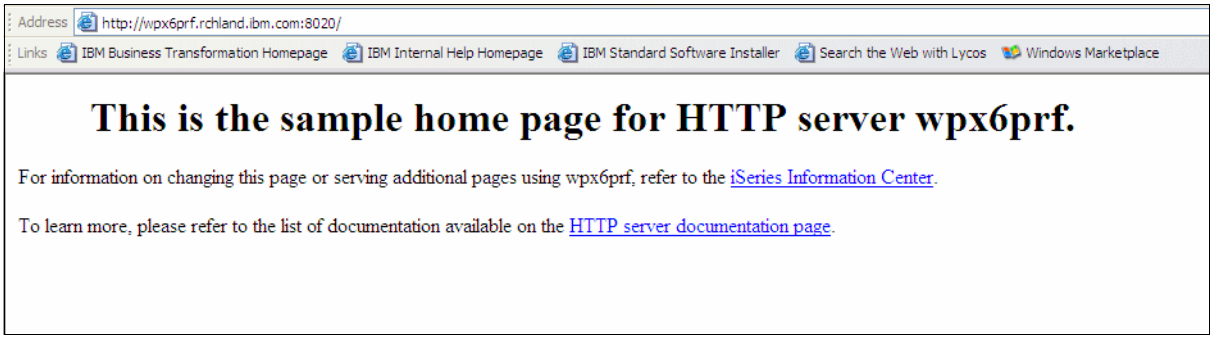

Address http://wpx6prf.rchland.ibm.com:8020/
Links IBM Business Transformation Homepage IBM Internal Help Homepage IBM Standard Software Installer Search the Web with Lycos Windows Marketplace
This is the sample home page for HTTP server wpx6prf.
For information on changing this page or serving additional pages using wpx6prf, refer to the iSeries Information Center.
To learn more, please refer to the list of documentation available on the HTTP server documentation page.

Figure 5-61 Checking the HTTP server configuration

2. To verify the SSL configuration of the HTTP Server, open a Web browser and enter the secure URL of the HTTP Server. In our example, this is `https://wpx6prf.rchland.ibm.com:8021`. If the configuration is correct, you see a pop-up window asking if you want to accept the key certificate for this Web site. See Figure 5-62. Click **Yes** to accept the key certificate.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate is from a trusted certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 5-62 Accepting the HTTP server certificate

3. You then see the default welcome page of the HTTP server (Figure 5-63).

Note: The protocol used is https, and a secure icon is displayed in the status line at the bottom of the Web browser window.

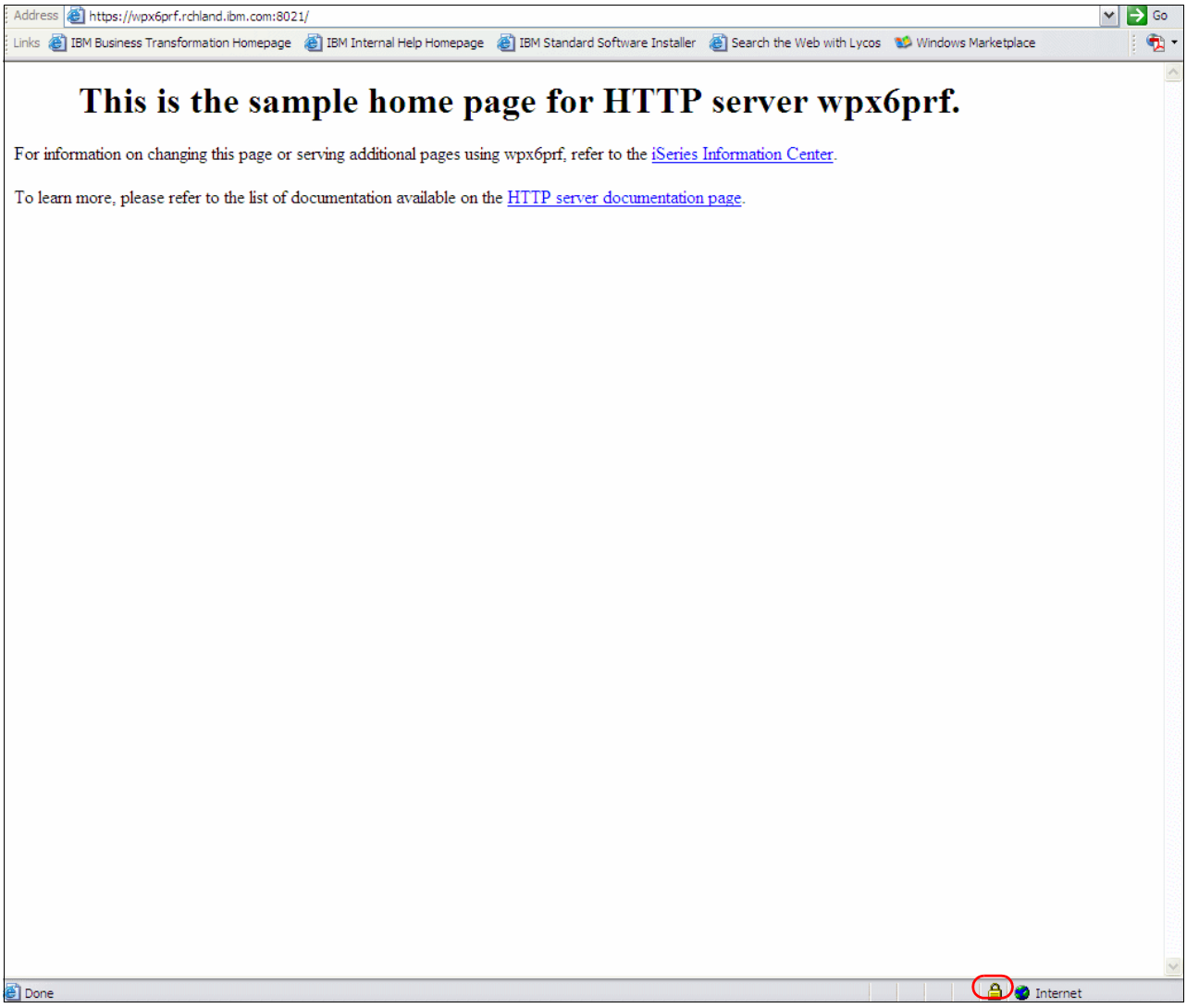

Address
https://wpx6prf.rchland.ibm.com:8021/
Go
Links
IBM Business Transformation Homepage
IBM Internal Help Homepage
IBM Standard Software Installer
Search the Web with Lycos
Windows Marketplace
This is the sample home page for HTTP server wpx6prf.
For information on changing this page or serving additional pages using wpx6prf, refer to the iSeries Information Center.
To learn more, please refer to the list of documentation available on the HTTP server documentation page.
Done
Internet

Figure 5-63 Checking the SSL configuration of the HTTP server

Your HTTP Server is now configured to accept SSL connections.

5.2.2 Enabling WebSphere Application Server for SSL

This section describes the configuration that is necessary to instantiate a secure connection between the HTTP server plugin and the internal HTTP transport in the Web container for the WebSphere Application Server. By default, this connection is not secure, even when global security is enabled on the WebSphere Application Server.

To configure the internal HTTP transport in the Web container of WebSphere Application Server to accept the SSL connections coming from the HTTP Server plugin, perform the following steps:

1. Create a self-signed certificate for the HTTP server plugin and import this certificate public key in the WebSphere Application Server Web container keystore.
2. Create a self-signed certificate for the WebSphere Application Server Web container and import this certificate into the HTTP server plugin keystore.
3. Modify the WebSphere Application Server Web container to support SSL with the certificates created in the two previous steps.

Note: In this section, we use the default trust and key stores for both the HTTP server plugin and WebSphere Application Server Web container. If you decide to use different stores, see the WebSphere Application Server for OS/400 V6 Information Center at:

http://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/topic/com.ibm.Websphere.iseries.doc/info/ae/ae/tsec_sslrep.html

The default key store file name for the HTTP Server plugin is plugin-key.kdb. The default key store file name for WebSphere Application Server Web container is DummyServerKeyFile.jks. The default trust store file name for WebSphere Application Server Web container is DummyServerTrustFile.jks. All three stores are located in the i5/OS integrate file system directory of /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/etc. For all three stores, the default password is WebAS and is case-sensitive.

The iKeyman utility tool

This section shows how to generate and exchange the certificates using the iKeyman utility tool. To learn more about this utility tool, see the iKeyman user manual at:

http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/50/GSK7c_SSL_IKM_Guide.pdf

Note: Because this tool uses a graphical user interface, you will need to map a network drive to your i5/OS integrated file system to access the key and trust stores of both the Web server plugin and the WebSphere Application Server Web container.

Creating and exchanging the self-signed certificates

This section show you how to create and exchange self-signed certificates.

Creating and extracting a certificate for the HTTP server plugin

Perform the following steps to create and extract a certificate for the HTTP server plugin:

1. To startup the iKeyman utility tool from your workstation, select **Start** → **Programs** → **IBM iSeries Access for Windows** → **IBM Key Management**. Figure 5-64 shows the iKeyman user interface.

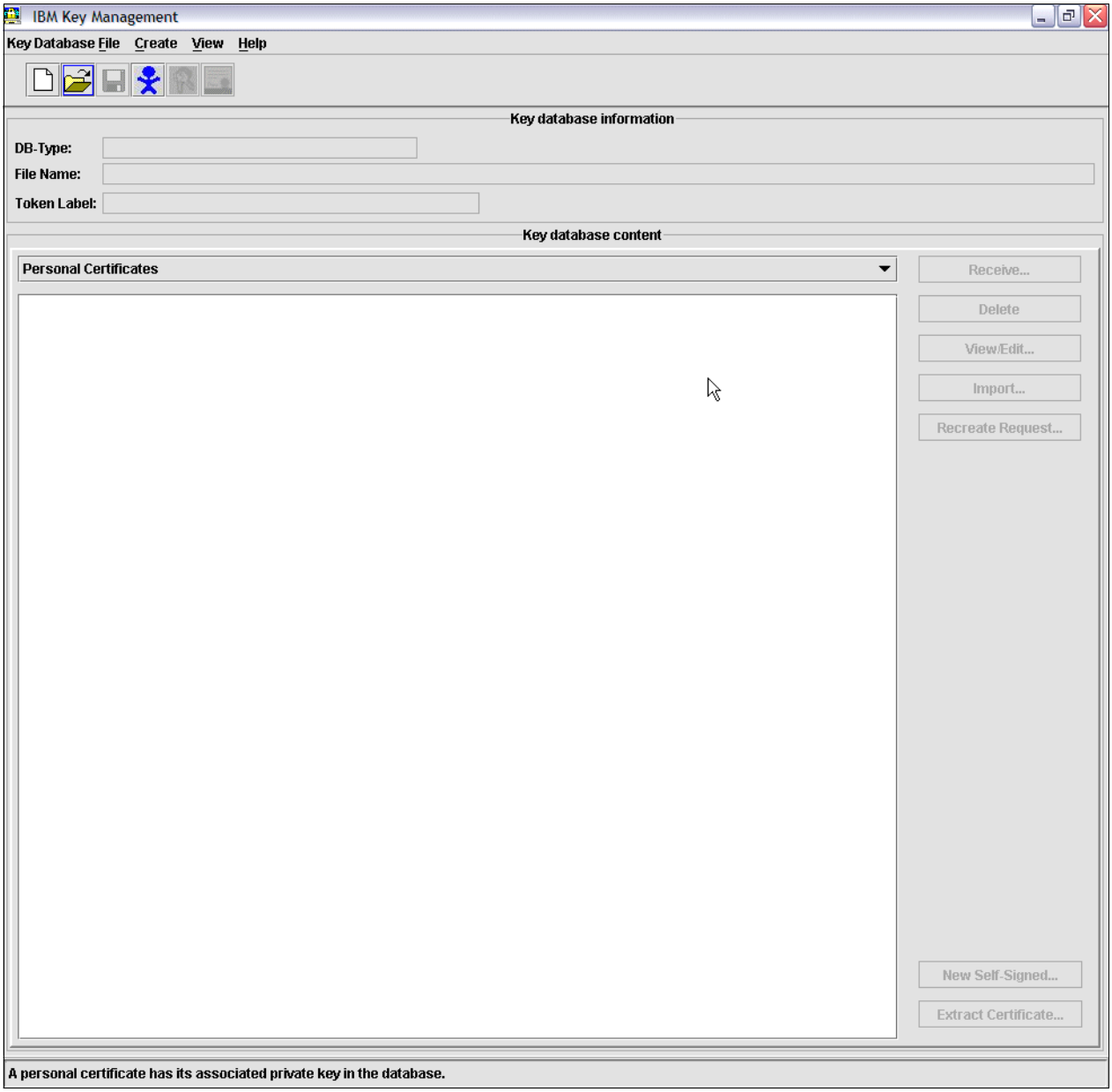


Figure 5-64 iKeyman utility tool interface

2. Open the HTTP Server plugin key store, plugin-key.kdb (Figure 5-65). Make sure you select **CMS** for the Key database type field. Click **OK**. Provide the key store password when requested.

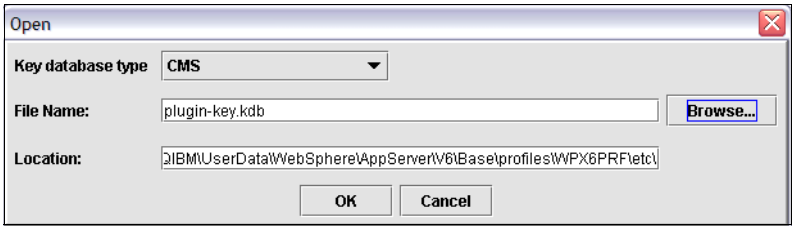


Figure 5-65 Opening the HTTP server plugin key store

3. From the menu, select **Create** → **New Self-Signed Certificate** (Figure 5-66).

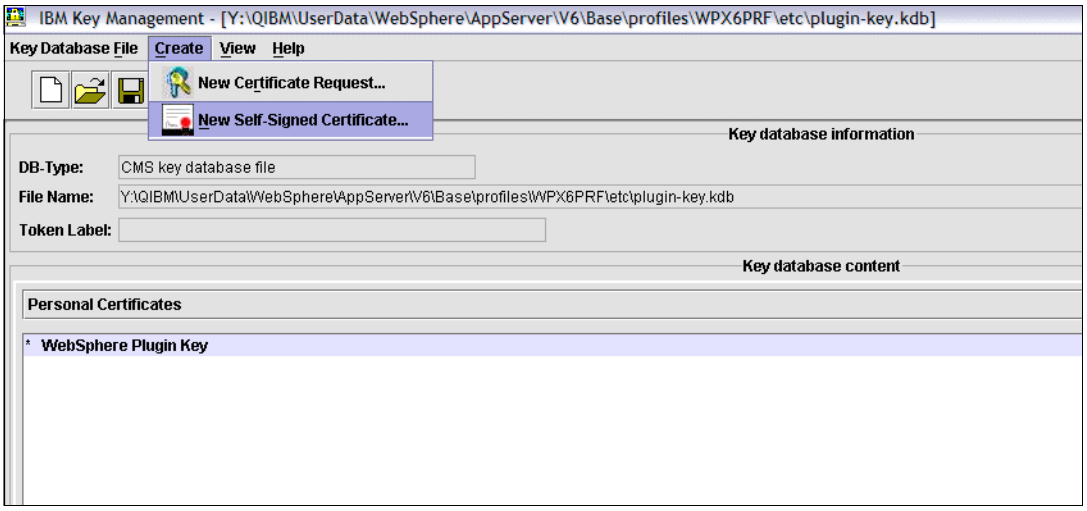


Figure 5-66 Creating a self-signed certificate for the HTTP server plugin

4. Fill in the certificate information (Figure 5-67). Keep track of the key label. In our example, it is `WebPlugin`. Click **OK** to save the certificate.

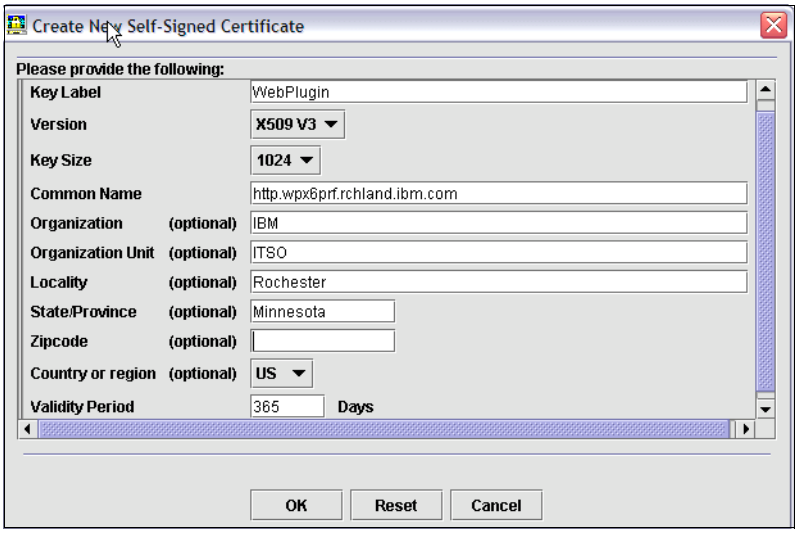


Figure 5-67 Filling in the HTTP server plugin certificate information

5. Click **Yes** when asked if you want to set the key as the default key (Figure 5-68).

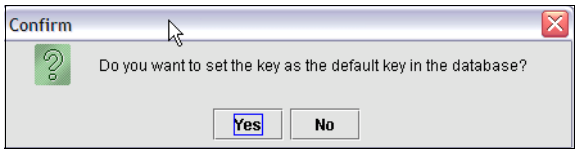


Figure 5-68 Setting the key as the default key

6. Select **Personal Certificates** from the Key database content field drop-down list, then select the certificate created in the previous step and click **Extract Certificate** (Figure 5-69).

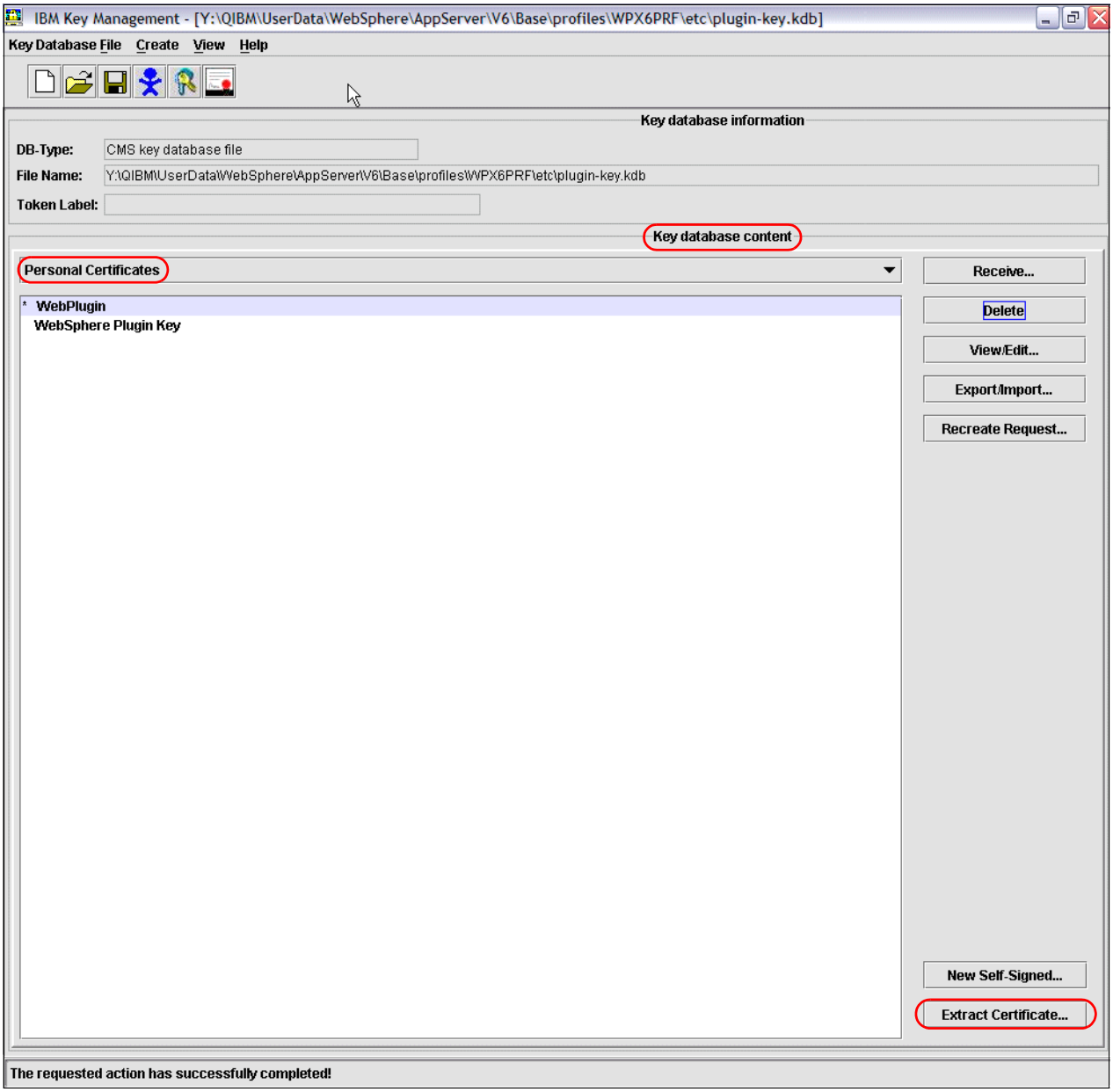


Figure 5-69 Extracting the certificate WebPlugin

7. Make sure you select **Base64-encoded ASCII data** for the Data type field. Save the certificate on your desktop. Name this file `WebPluginPubCert.arm` (Figure 5-70).

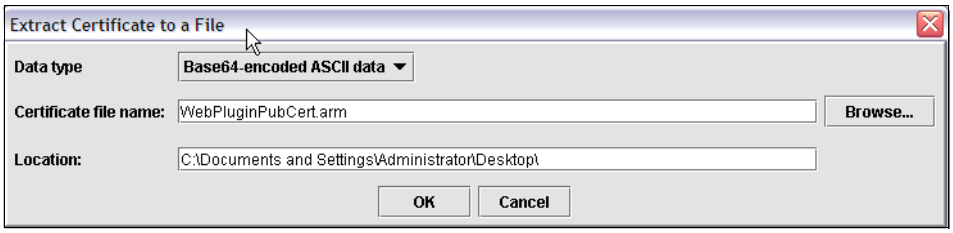


Figure 5-70 Saving the extracted certificate to your desktop

Creating and extracting the certificate for the Application Server Web container

Perform the following steps to create and extract the certificate for the WebSphere Application Server Web Container:

1. Open the WebSphere Application Server key store, DummyServerKeyFile.jks (Figure 5-71). Make sure you select **JKS** for the Key database type field. Click **OK**. Provide the key store password when requested.

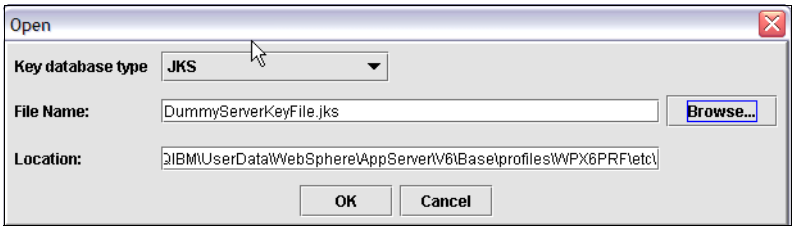


Figure 5-71 Opening the WebSphere Application Server Web container key store

2. From the menu, select **Create** → **New Self-Signed Certificate** (Figure 5-72).

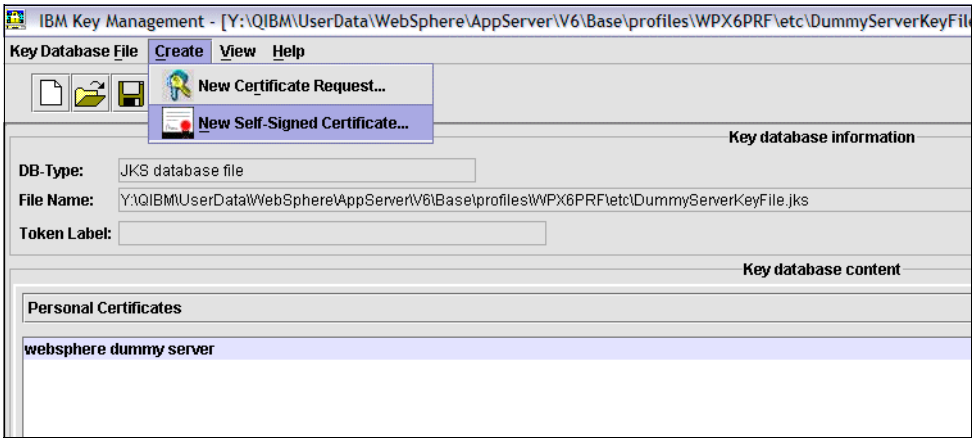


Figure 5-72 Creating a self-signed certificate for the WebSphere Application Server Web container

3. Fill in the certificate information (Figure 5-73). Keep track of the key label. In our example, it is `WASWebContainer`. Click **OK** to save the certificate.

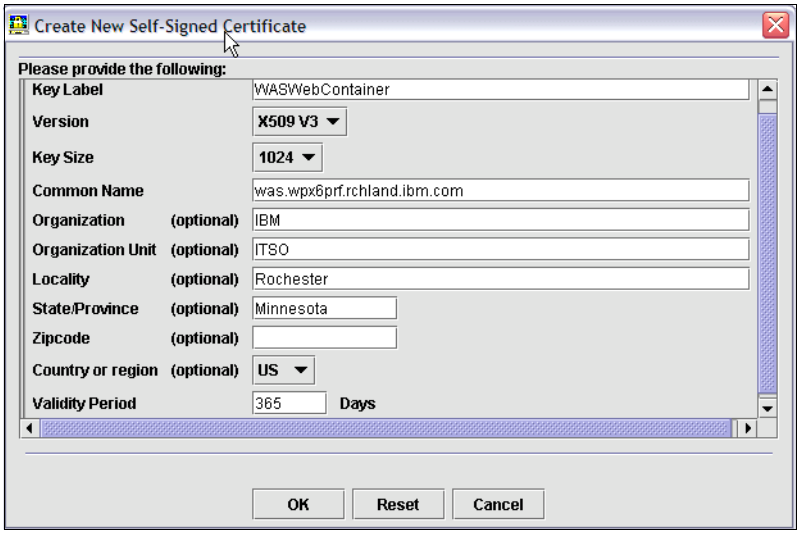


Figure 5-73 Filling in the Application Server Web container certificate information

4. Select **Personal Certificates** from the Key database content field drop-down list, then select the certificate created in the previous step and click **Extract Certificate** (Figure 5-74).

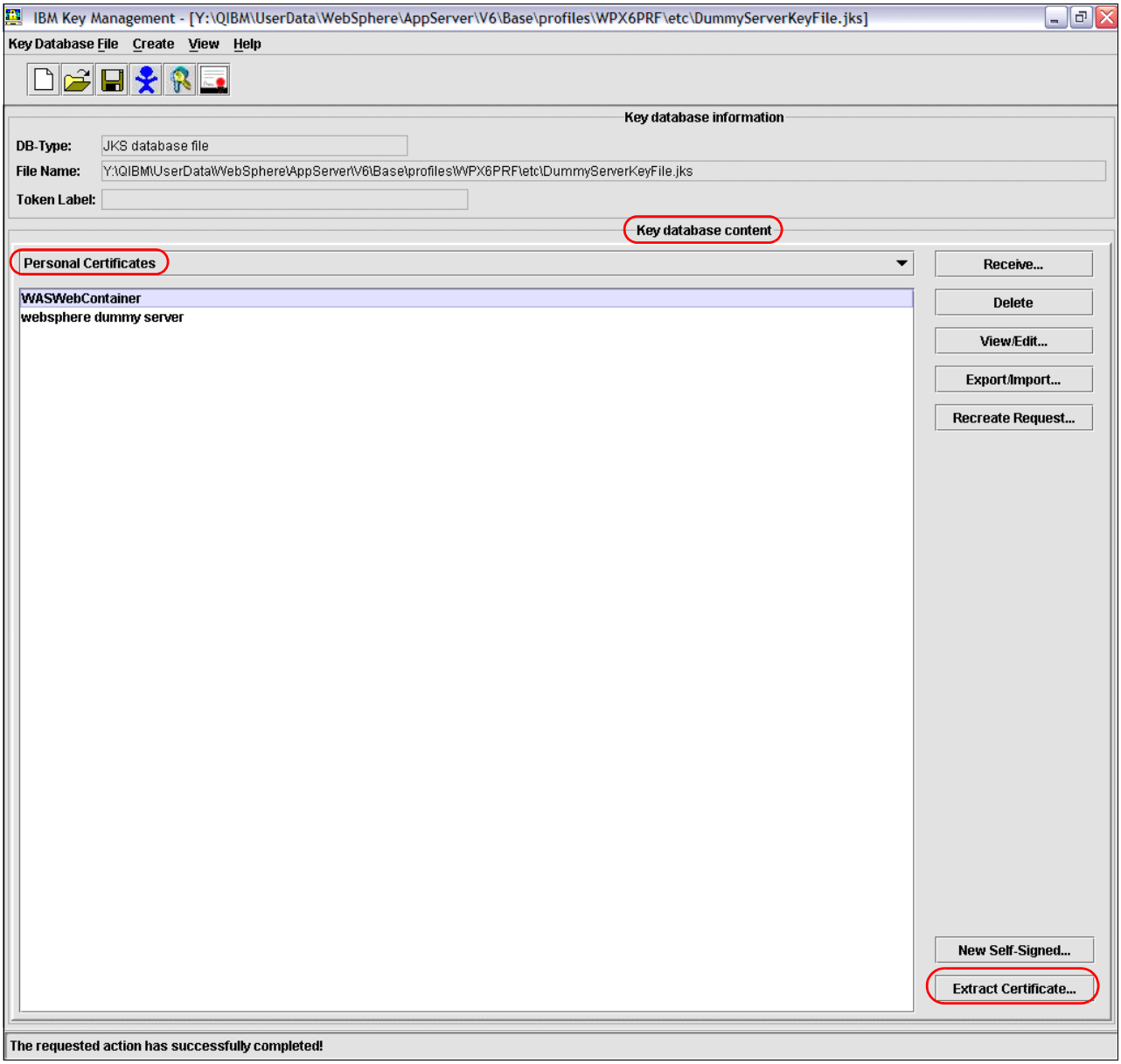


Figure 5-74 Extracting the certificate WASWebContainer

5. Select **Base64-encoded ASCII data** for the Data type field. Save the certificate on your desktop. Name this file `WASWebContainerPubCert.arm` (Figure 5-75). Click **OK**.

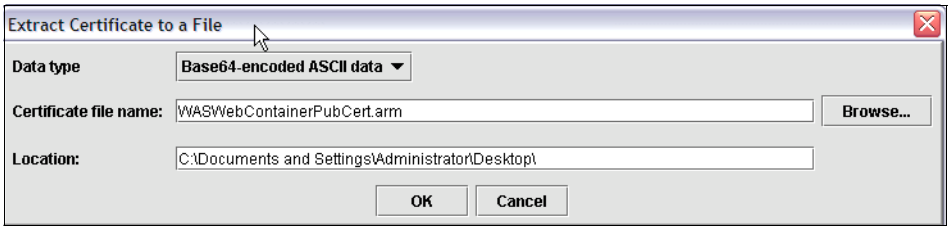


Figure 5-75 Saving the extracted certificate to your desktop

6. Select **Signer Certificates** from the Key database content field drop-down list and click **Add** (Figure 5-76).

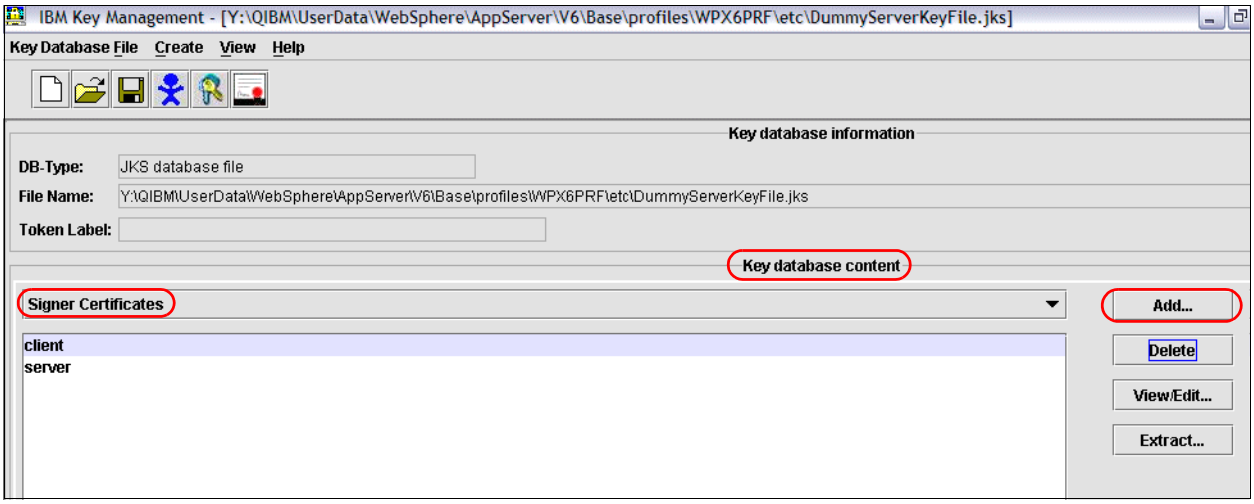


Figure 5-76 Selecting the Signer Certificates section of the store

7. Import the extracted certificate, WASWebContainerPubCert.arm, in the signer section of the store (Figure 5-77). Click **OK**.

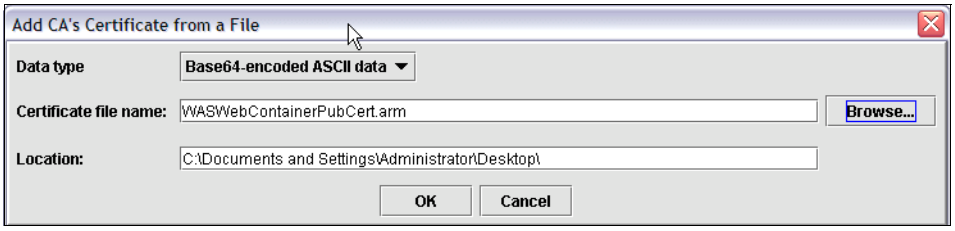


Figure 5-77 Adding the CA of the certificate to the signer section of the store

8. Enter a label for the CA when prompted. In our example, this is `WASWebContainerSigner`. Click **OK** (Figure 5-78).

Figure 5-78 Labeling the certificate CA

9. Open the WebSphere Application Server Web container trust store DummyServerTrustFile.jks. Make sure you select **JKS** for the Key database type field. Provide the trust store password when requested. Then repeat Steps 6 and 7 of “Creating and extracting the certificate for the Application Server Web container” on page 203 to import the WASWebContainerPubCert.arm CA into the trust store.

Exchanging certificates

Perform the following steps to exchange certificates:

1. Open the HTTP Server plugin key store plugin-key.kdb. Make sure you select **CMS** for the Key database type field. Provide the key store password when requested.

2. Select **Signer Certificates** from the Key database content field drop-down list, then click **Add** to import the extracted certificate WASWebContainerPubCert.arm in the signer section of the store. Enter `WASWebContainerSigner` when prompted for the label.
3. Open the WebSphere Application Server Web container key store DummyServerKeyFile.jks. Make sure you select **JKS** for the Key database type field. Provide the key store password when requested.
4. Select **Signer Certificates** from the Key database content field drop-down list, then click **Add** to import the extracted certificate, WebPluginPubCert.arm, in the signer section of the store. Enter `WebPluginSigner` when prompted for the label.
5. Close the iKeyman utility tool. You are now finished with the certificate work.

Configuring the WebSphere Application Server to support SSL

Perform the following steps to configure the WebSphere Application Server to support SSL:

1. Open a Web browser and log in to the WebSphere Administration console.
2. In the left navigation pane, expand **Security** and click **SSL**. In the right pane, click **New JSSE Repertoire** (Figure 5-79).

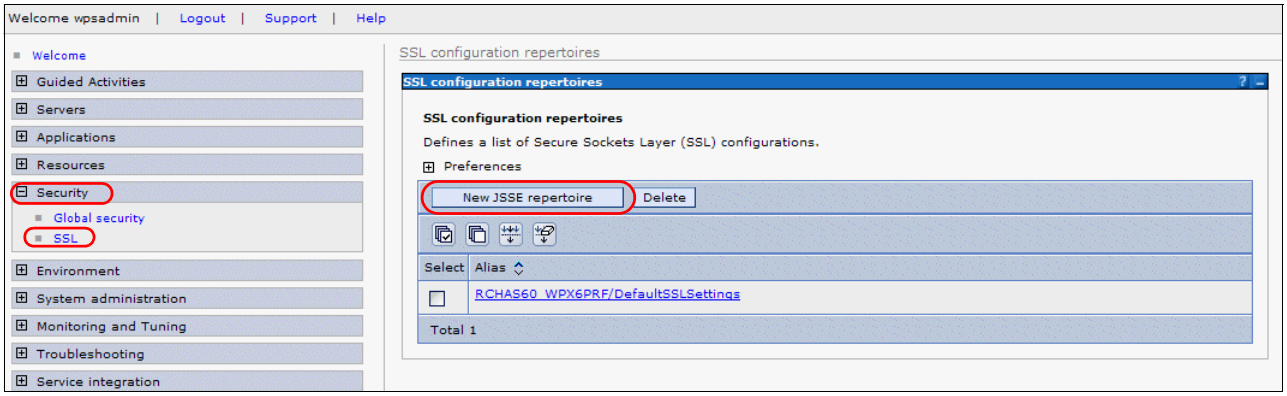


Figure 5-79 Creating a new entry in the SSL configuration repertoire

3. Fill in the information from Table 5-1 as shown on Figure 5-80 on page 208.

Table 5-1 Parameters for creating a new entry in the SSL configuration repertoire

Parameter	Value
Alias	WebContainerSSLSettings
Security level	HIGH
Key file name	/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/etc/DummyServerKeyFile.jks
Key file password	WebAS
Key file format	JKS
Trust file name	/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/etc/DummyServerTrustFile.jks
Trust file password	WebAS
Trust file format	JKS

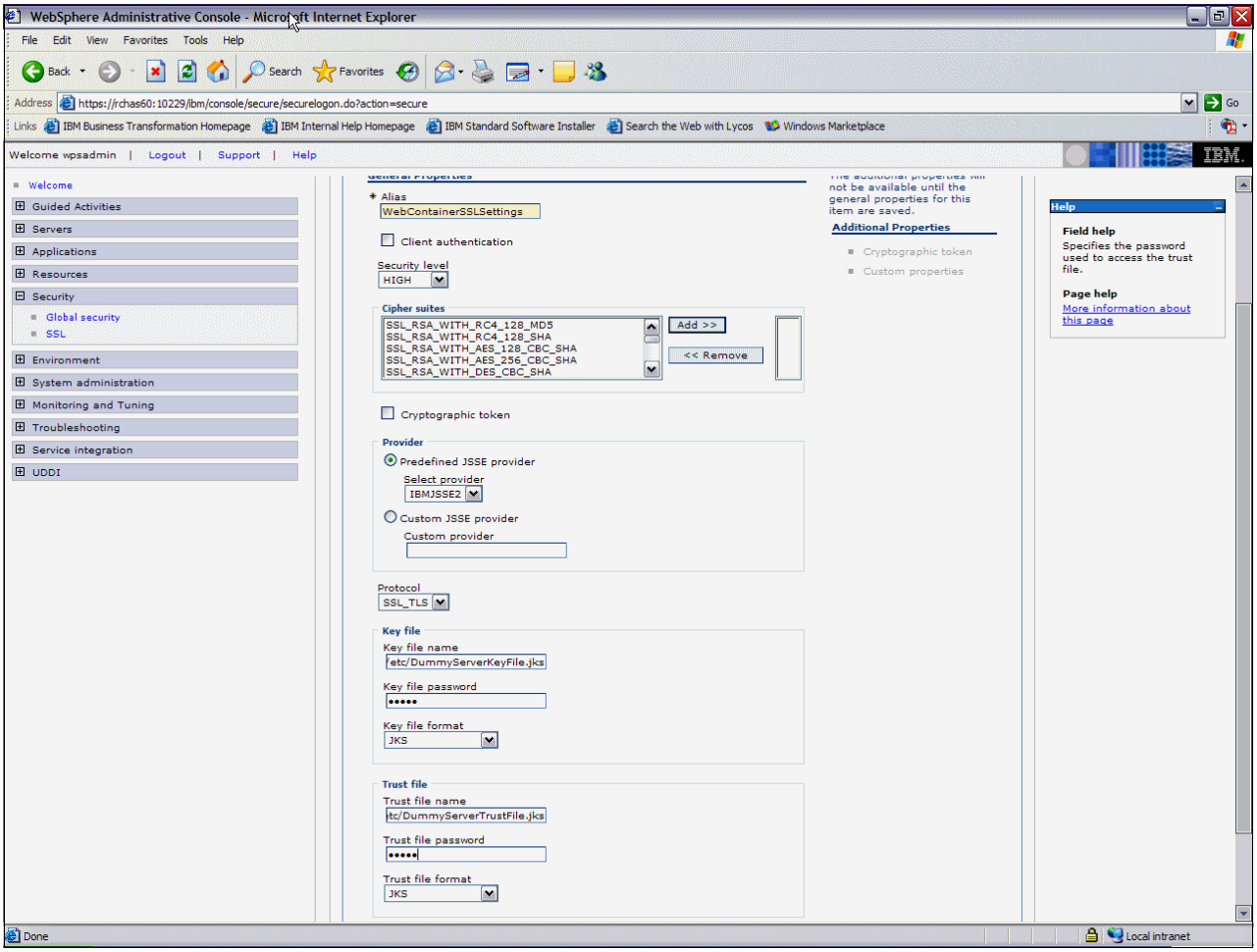


Figure 5-80 Setting up a new entry in the SSL configuration repertoire

4. Click **OK** and save the changes to the master configuration file.
5. In the left navigation pane, expand **Servers** and click **Application Servers**, then in the right pane, click **WebSphere_Portal** (Figure 5-81).

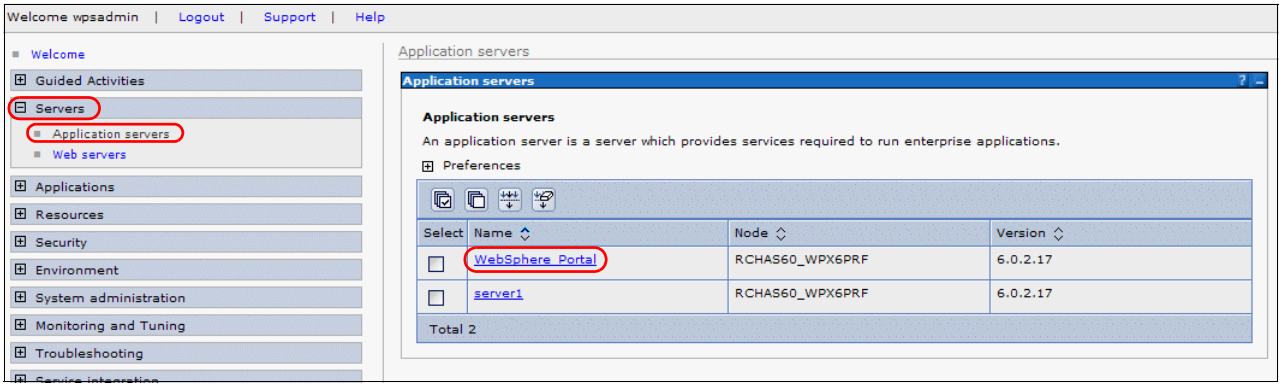


Figure 5-81 Managing WebSphere_Portal server

6. Under **Container Settings**, expand **Web Container Settings** and click **Web container transport chains** (Figure 5-82).

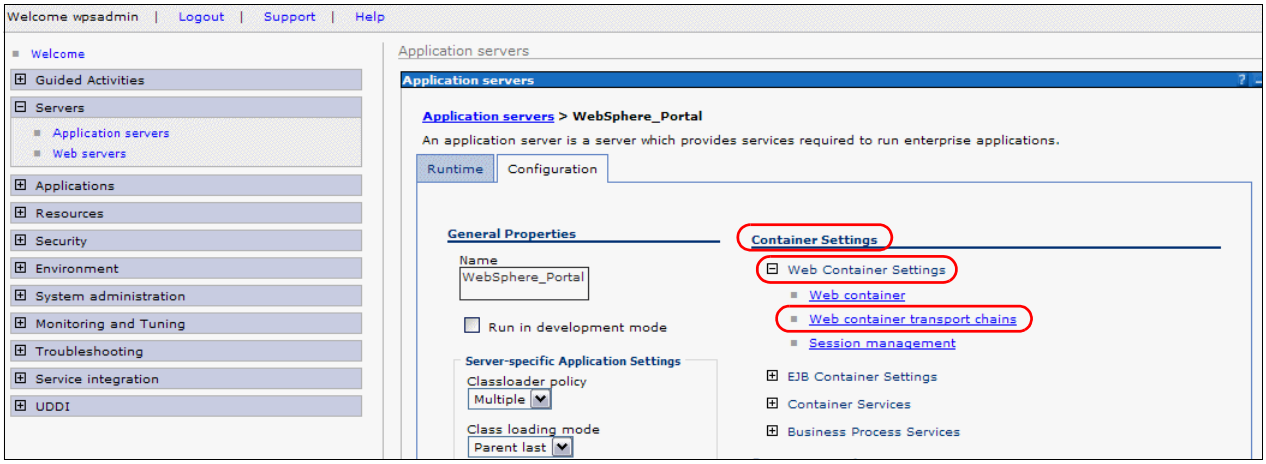


Figure 5-82 Managing Web container transport chains

7. Click **WCInboundDefaultSecure** (Figure 5-83).

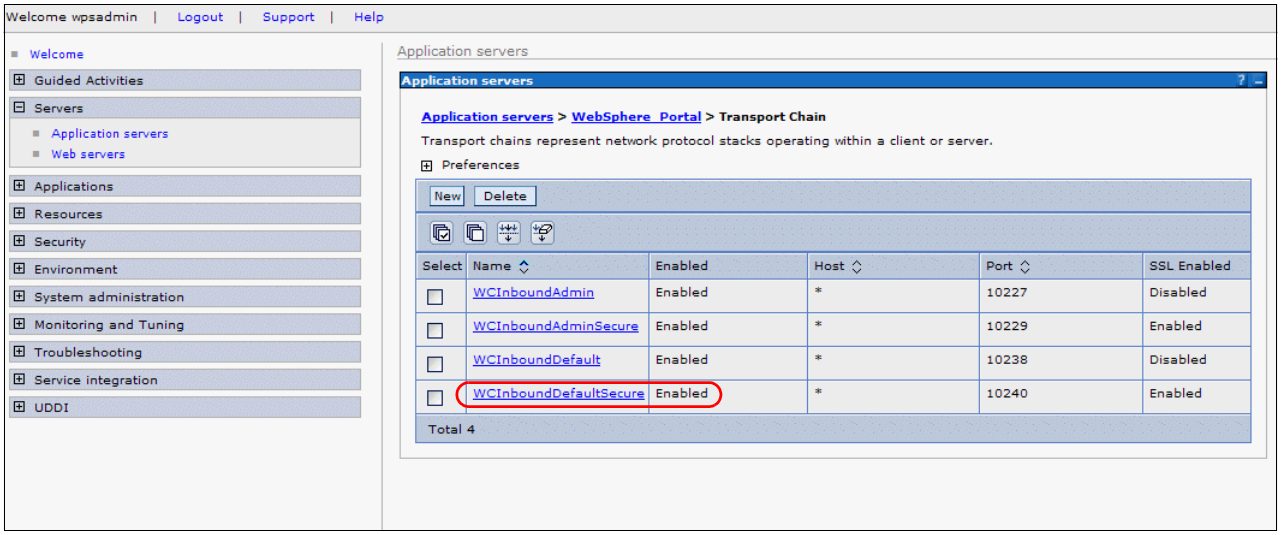


Figure 5-83 Managing Web container secure transport chain

8. Click **SSL Inbound Channel (SSL_2)** (Figure 5-84).

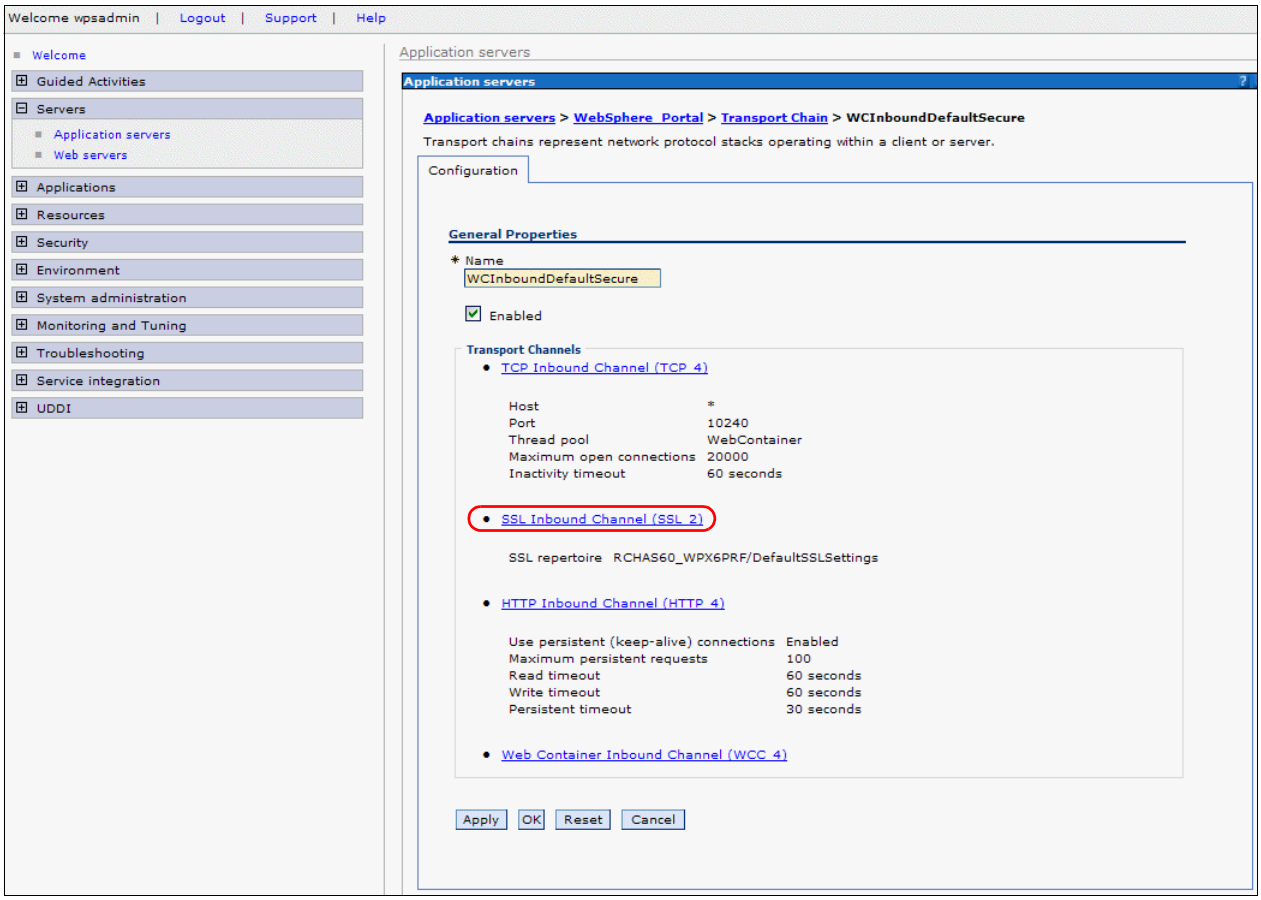


Figure 5-84 Setting up the SSL transport chain

9. From the drop-down list, select the new JSSE Repertoire entry created in Step 1 of this section. The alias is WebContainerSSLSettings (Figure 5-85).

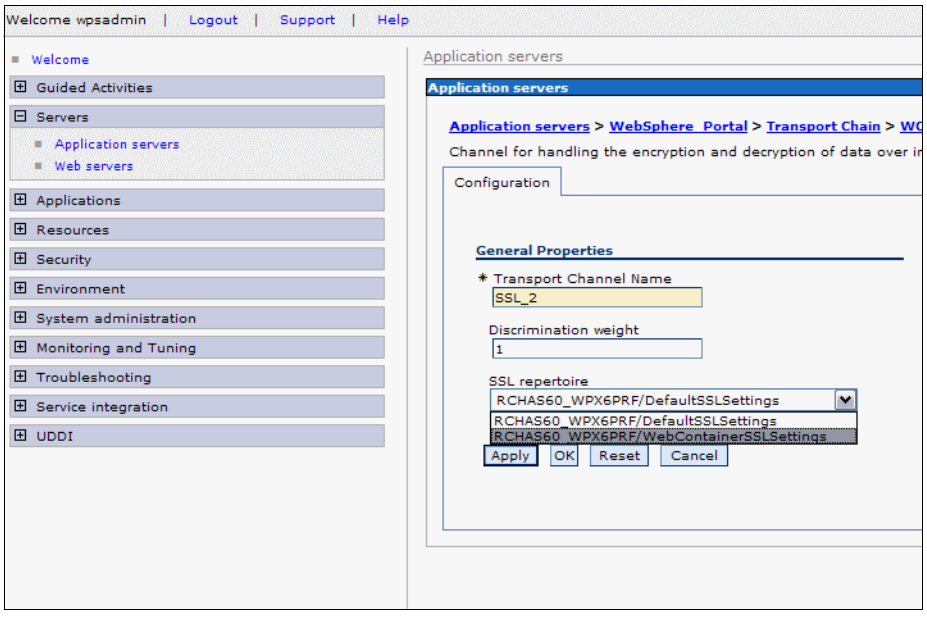


Figure 5-85 Selecting the JSSE repertoire entry

10. Click **OK** and save the changes to the master configuration file.

11. In the left navigation pane, expand **Environment**, click **Virtual Hosts**, then in the right pane, click **default_host** (Figure 5-86).

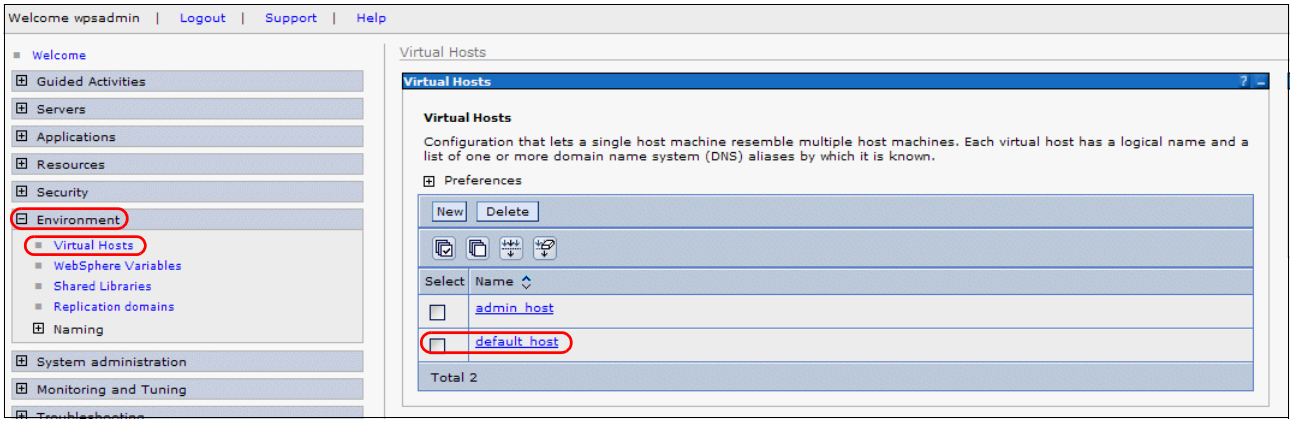


Figure 5-86 Managing the default virtual host

12. Click **Host Aliases** (Figure 5-87).

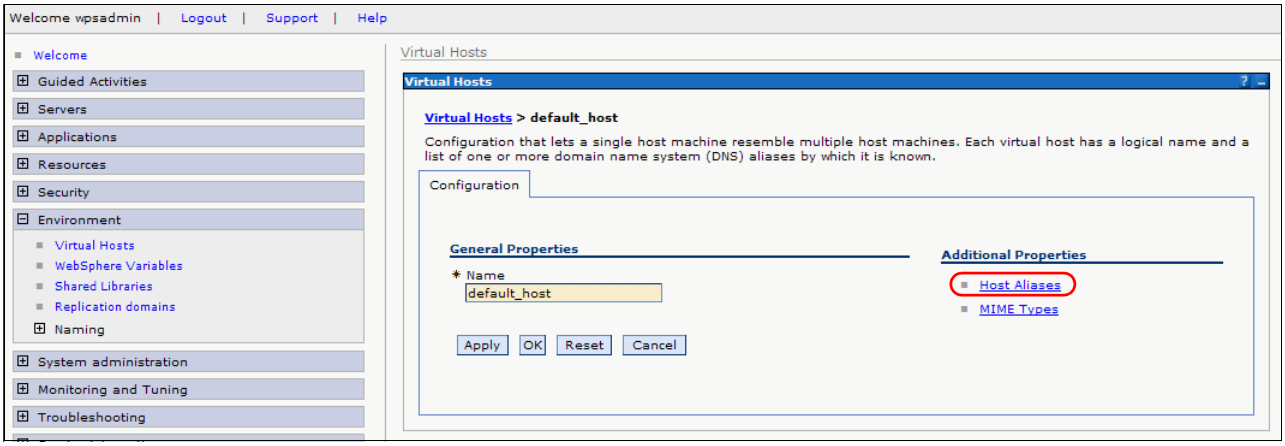


Figure 5-87 Managing host aliases

13. Check that there is an entry for the Web container secure port (Figure 5-88). If it is missing, add it, and then save the changes to the master configuration file.

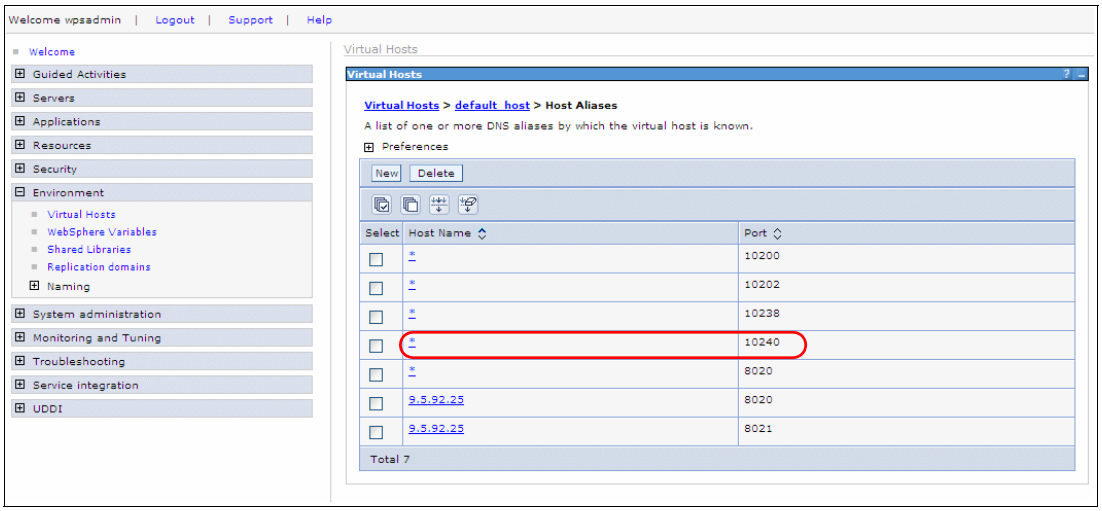


Figure 5-88 Host aliases for the Web container

If you do not remember the port number, check it from the IBM Web Administration for i5/OS interface. Select the **Manage** tab, then the **Application Servers** tab. Select your WebSphere Application Server from the drop-down list, and in the left navigation pane under **Server Properties**, click **Server Ports** (Figure 5-89).

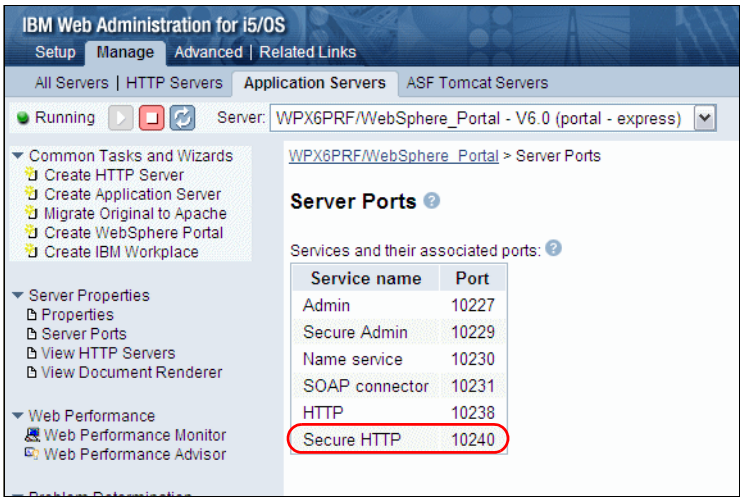


Figure 5-89 Finding out the Web container secure port

14. Also check that there are entries for the external HTTP server ports, both secure and non-secure (Figure 5-90). If they are missing, add them, and then save the changes to the master configuration file.

    If you do not remember the port numbers, check them from the IBM Web Administration for I5/OS interface.

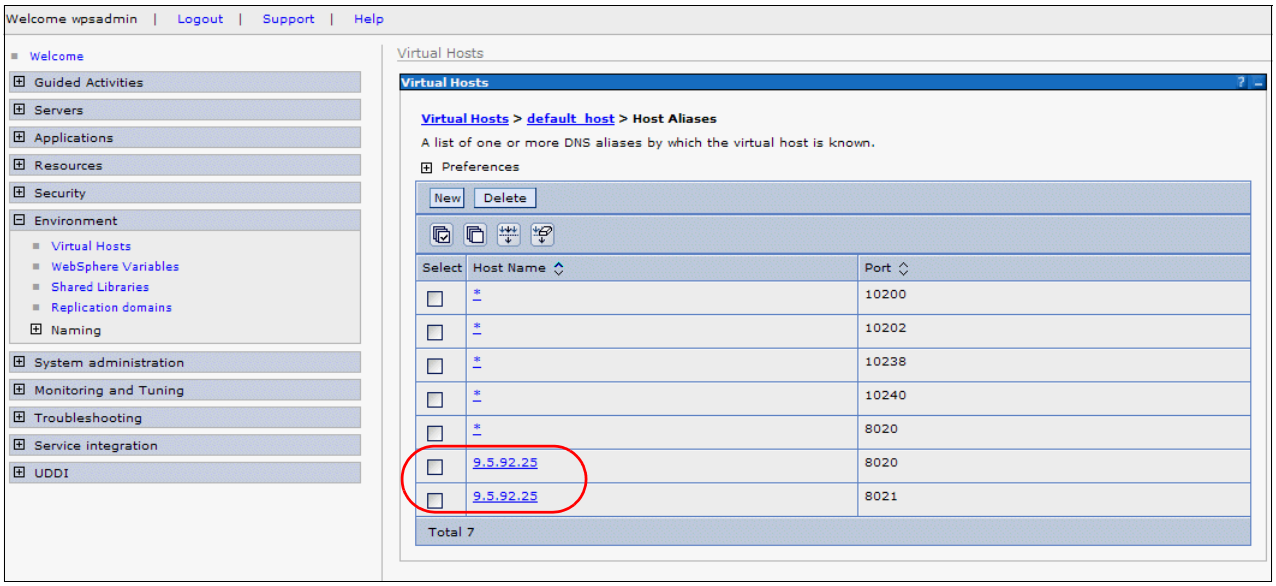


Figure 5-90 Host aliases for the external HTTP server

15. In the left navigation pane, expand **Servers**, click **Web Servers**, then in the right pane, click the Web server name, **IHS_RCHAS60_WPX6PRF**, as in our example (Figure 5-91).

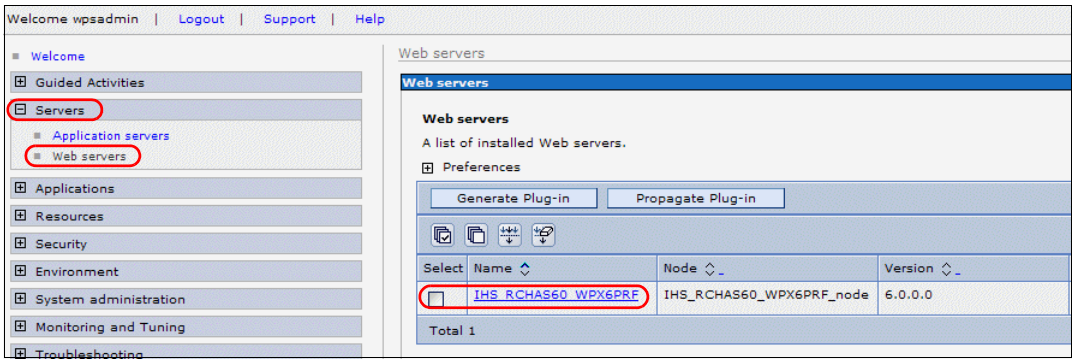


Figure 5-91 Managing the Web server plugin

16. Under **Additional Properties**, click **Plugin Properties** (Figure 5-92).

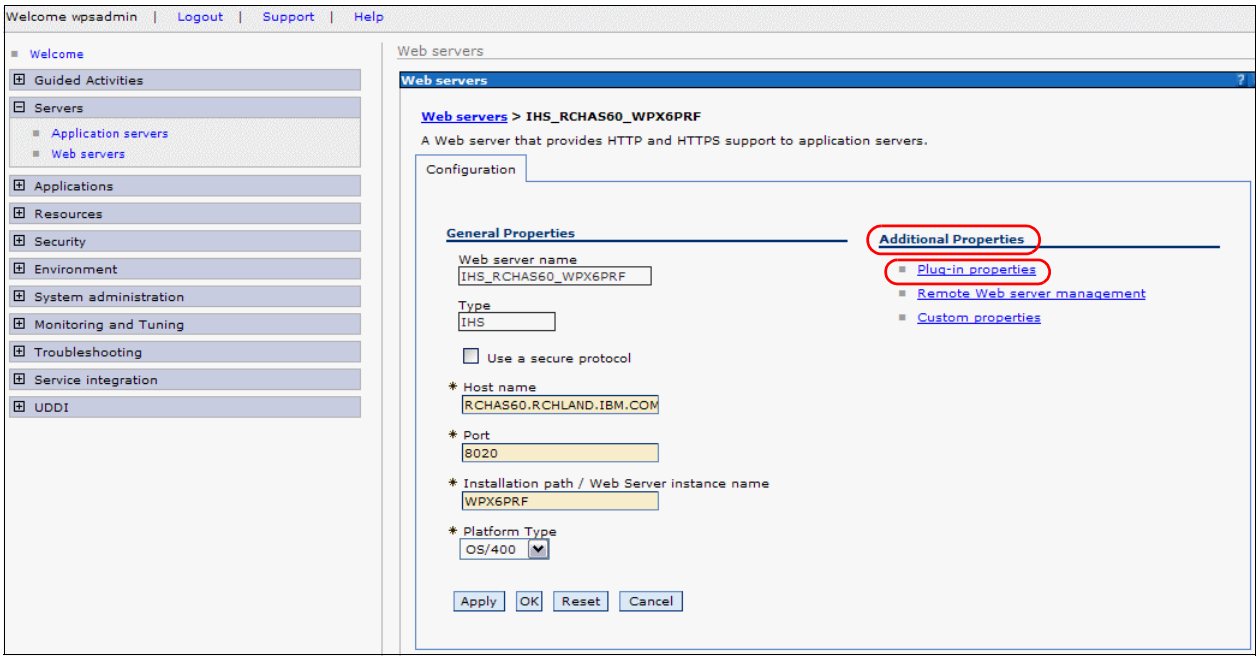


Figure 5-92 Plugin properties

17. Click **Custom Properties** (Figure 5-93).

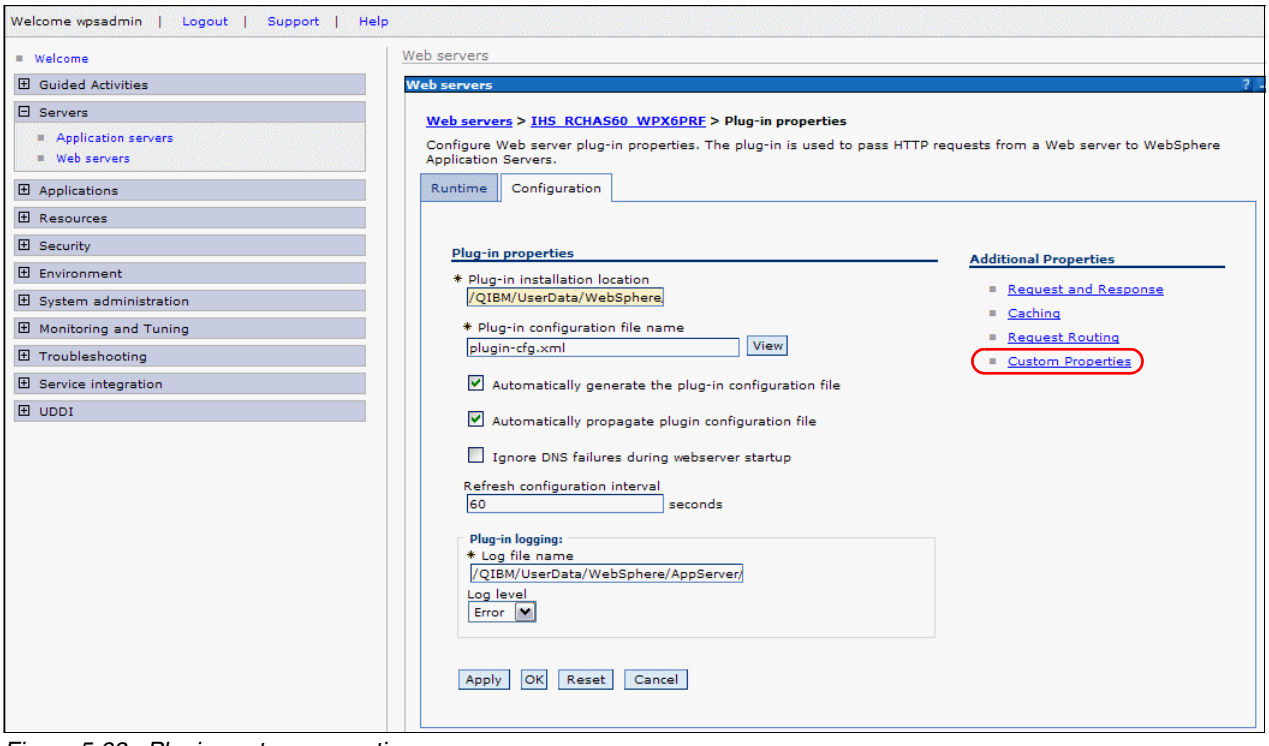


Figure 5-93 Plugin custom properties

18. Create the following properties from Table 5-2 as shown in Figure 5-94.

Table 5-2 Plugin custom properties for SSL

Property	Value
KeyringLocation	/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/etc/plugin-key.kdb
StashfileLocation	/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/etc/plugin-key.sth

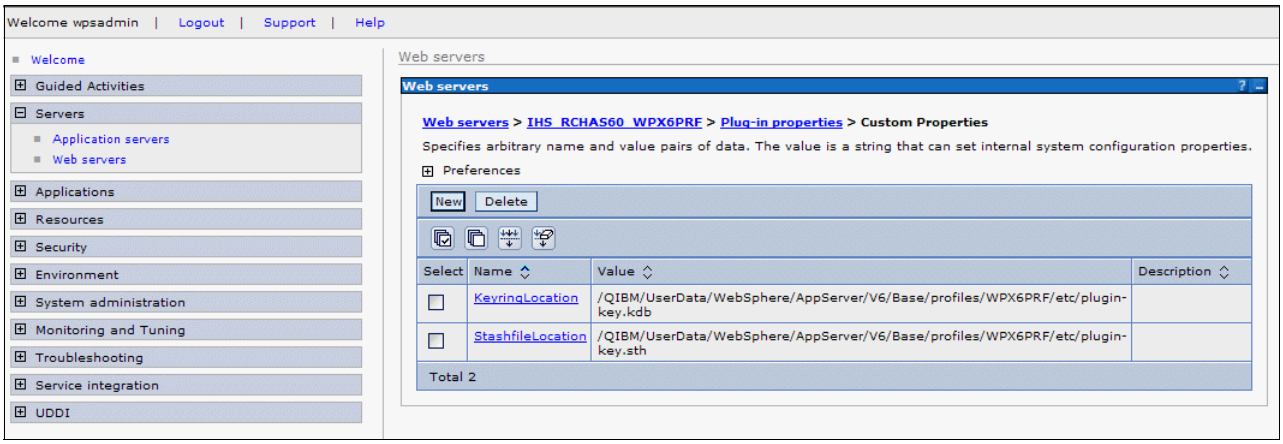


Figure 5-94 Plugin custom properties for SSL

19. Save the changes to the master configuration file.
20. Log out from the WebSphere Administration console. Do *not* restart WebSphere Application Server at this point.
21. Edit the file soap.client.props located in the i5/OS integrated file system directory of /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/properties.

> **Tip:** Create a copy of this file and keep the copy safe before you modify it.

22. Update the properties file com.ibm.ssl.trustStore with the fully qualified path of the Web container trust store (`DummyServerTrustFile.jks` in our example).
23. Update the property file com.ibm.ssl.trustStorePassword with the password of the Web container trust store (`WebAS` in our example).
24. Update the properties file com.ibm.ssl.keyStore with the fully qualified path of the Web container key store (`DummyServerKeyFile.jks` in our example).
25. Update the property file com.ibm.ssl.keyStorePassword with the password of the Web container key store (`WebAS` in our example).
26. Save the changes (Figure 5-95 on page 216).

```
#-------------------------------------------------------------------------------
# SSL Configuration
#
# - keyStore and trustStore                     (fully qualified path to file)
# - keyStorePassword and trustStorePassword     (string specifying password -
encoded or not)
#-------------------------------------------------------------------------------
com.ibm.ssl.keyStore=/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WPX6PR
F/etc/DummyServerKeyFile.jks
com.ibm.ssl.keyStorePassword=WebAS
com.ibm.ssl.trustStore=/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WPX6
PRI/etc/DummyServerTrustFile.jks
com.ibm.ssl.trustStorePassword=WebAS
com.ibm.ssl.contextProvider=IBMJSSE2
# use contextProvider below for FIPS
# com.ibm.ssl.contextProvider=IBMJSSEFIPS
```

Figure 5-95 Updating the soap.client.props file

27. If you have modified the password for any of the stores, you need to run the password encoder utility for security reasons. From the Qshell command line, enter the following commands:

    ```
    /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/portal_profile/bin/PropFile
    PasswordEncoder

    /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/portal_profile/properties/s
    oap.client.props property_name
    ```

    Where *property_name* is the property name of the password to encode:

    - *com.ibm.ssl.keyStorePassword* for the Web container key store password
    - *com.ibm.ssl.trustStorePassword* for the Web container trust store password

28. Check that the passwords are encrypted. See Figure 5-96.

```
#-------------------------------------------------------------------------------
# SSL Configuration
#
# - keyStore and trustStore                     (fully qualified path to file)
# - keyStorePassword and trustStorePassword     (string specifying password -
encoded or not)
#-------------------------------------------------------------------------------
com.ibm.ssl.keyStore=/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WPX6PR
F/etc/DummyServerKeyFile.jks
com.ibm.ssl.keyStorePassword={xor}CDo9Hgw\=
com.ibm.ssl.trustStore=/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WPX6
PRI/etc/DummyServerTrustFile.jks
com.ibm.ssl.trustStorePassword={xor}CDo9Hgw\=
com.ibm.ssl.contextProvider=IBMJSSE2
# use contextProvider below for FIPS
# com.ibm.ssl.contextProvider=IBMJSSEFIPS
```

Figure 5-96 Encrypted passwords

29. Stop and restart WebSphere Application Server.

5.2.3 Enabling WebSphere Portal Express for SSL: login only

This section describes the steps to only encrypt the login process for the portal. When the user authentication is done, no portal pages are encrypted. If the content you want to display is critical to your business or is confidential, you need to consider encrypting all portal pages. In this case, see 5.2.4, “Enabling WebSphere Portal Express for SSL: All pages” on page 227.

1. Open a Web browser and log in to the WebSphere Administration console.
2. In the left navigation pane, expand **Resources** and select **Resource Environment Provider**, then in the right pane, click **WP_ConfigService** (Figure 5-97).

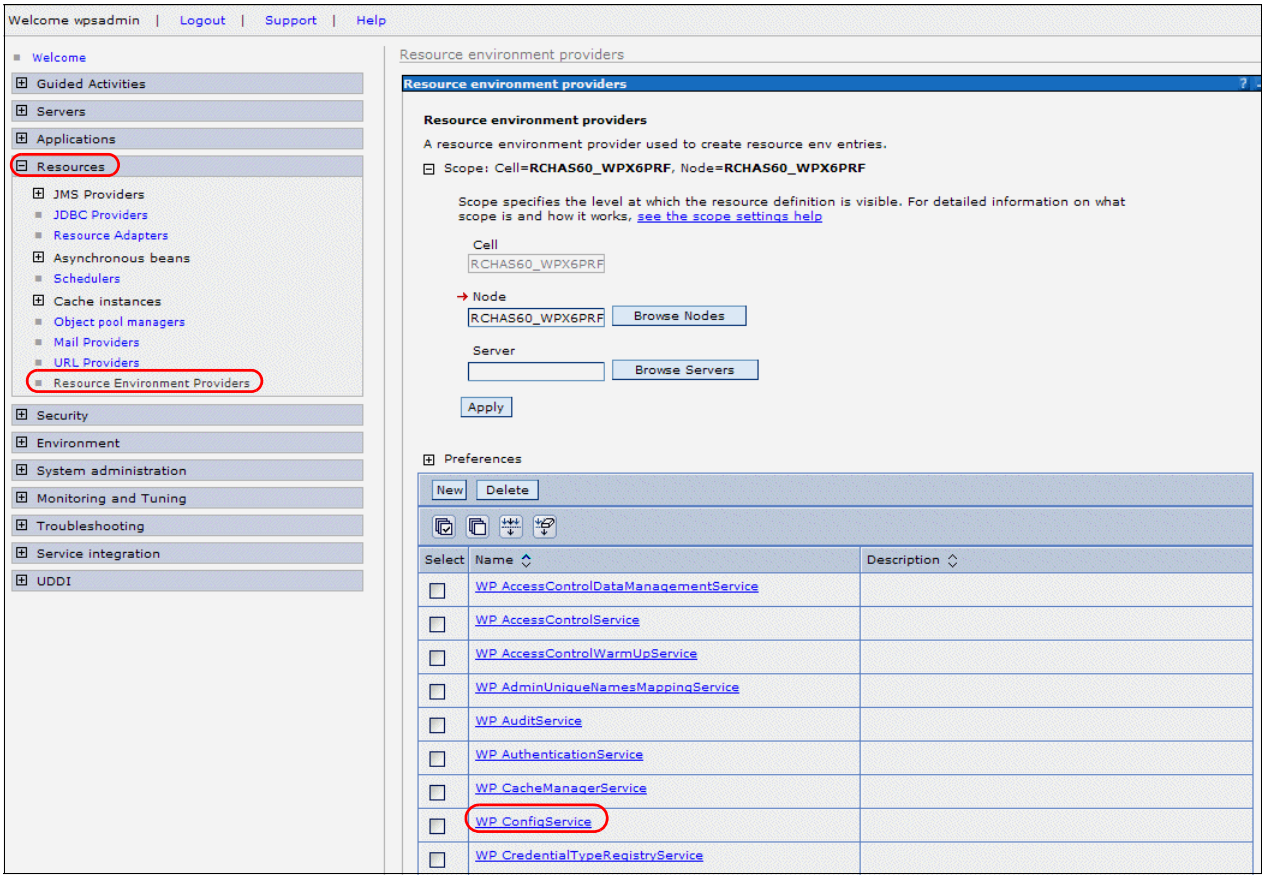


Figure 5-97 Accessing the portal service ConfigService

3. Click **Custom properties** (Figure 5-98).

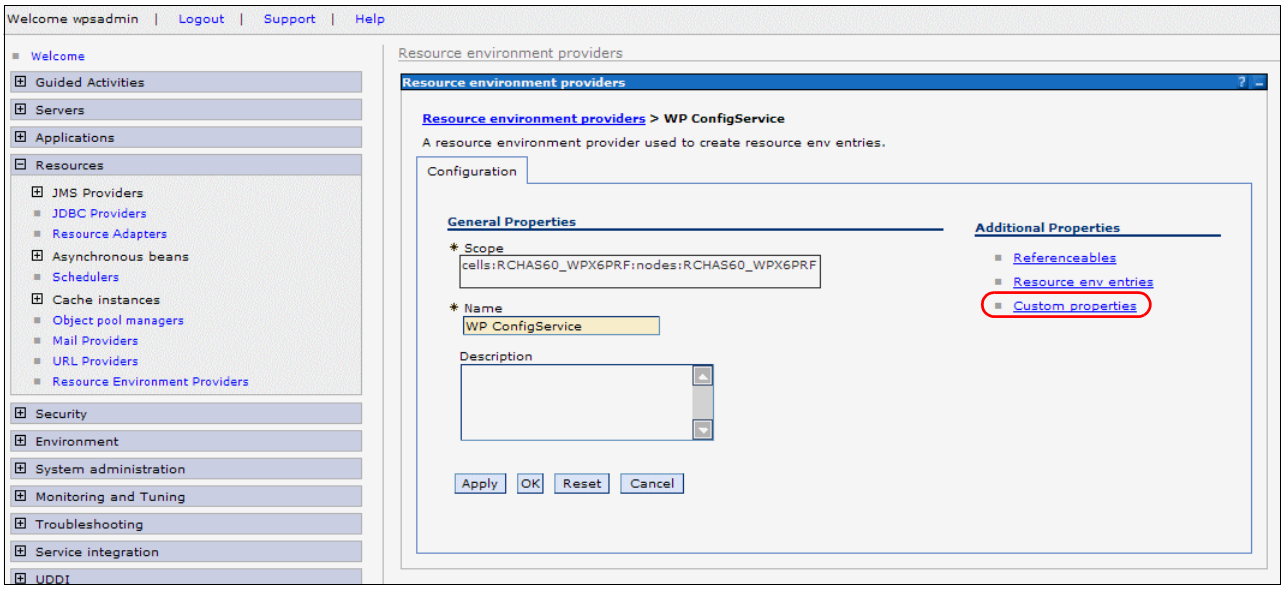


Figure 5-98 Portal service ConfigService custom properties

4. Set the custom property *host.port.http* to the value of the external HTTP Server non-secure port (Figure 5-99).

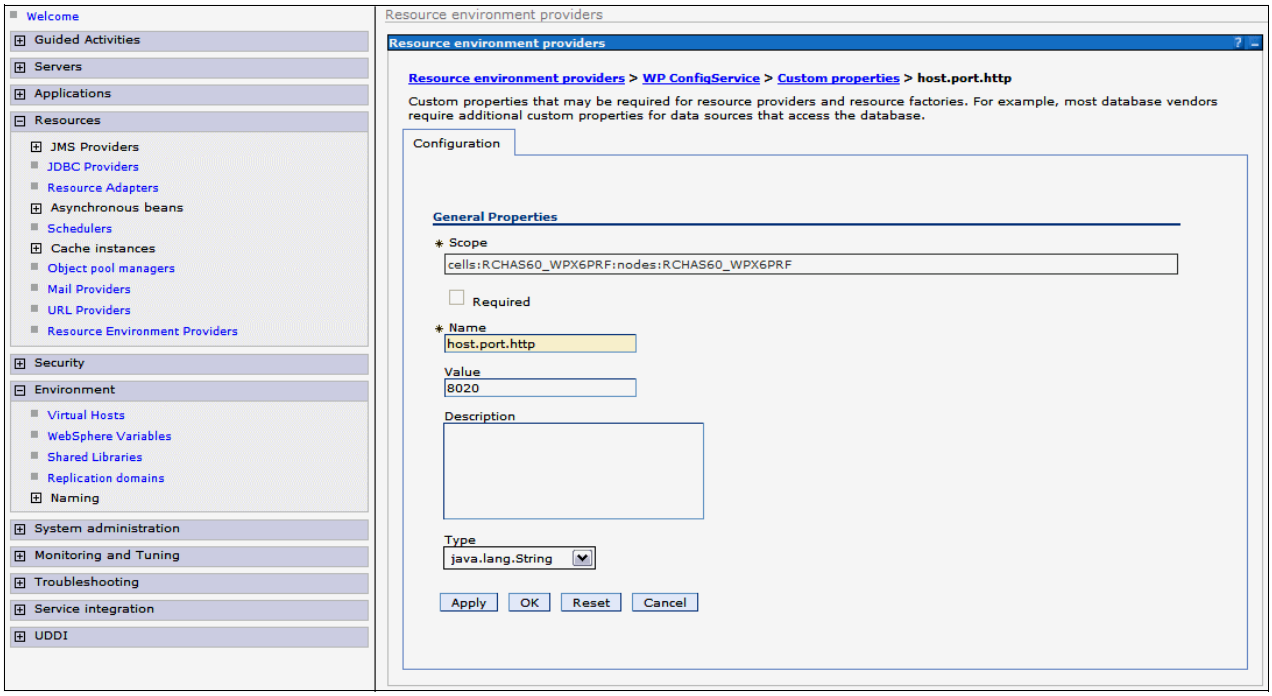


Figure 5-99 Custom property of host.port.http

5. Set the custom property *host.port.https* to the value of the external HTTP Server secure port (Figure 5-100).

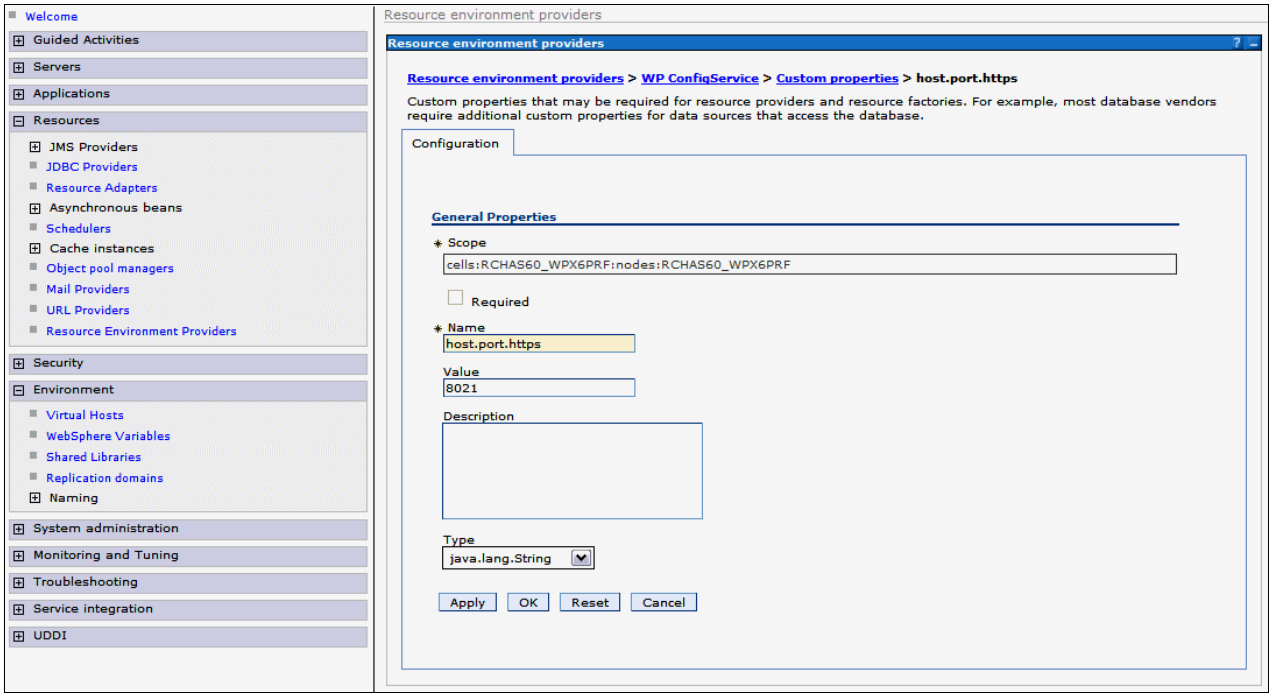


Figure 5-100 Custom property of host.port.https

6. Add the custom property *redirect.login.ssl* and set its value to **false** (Figure 5-101).

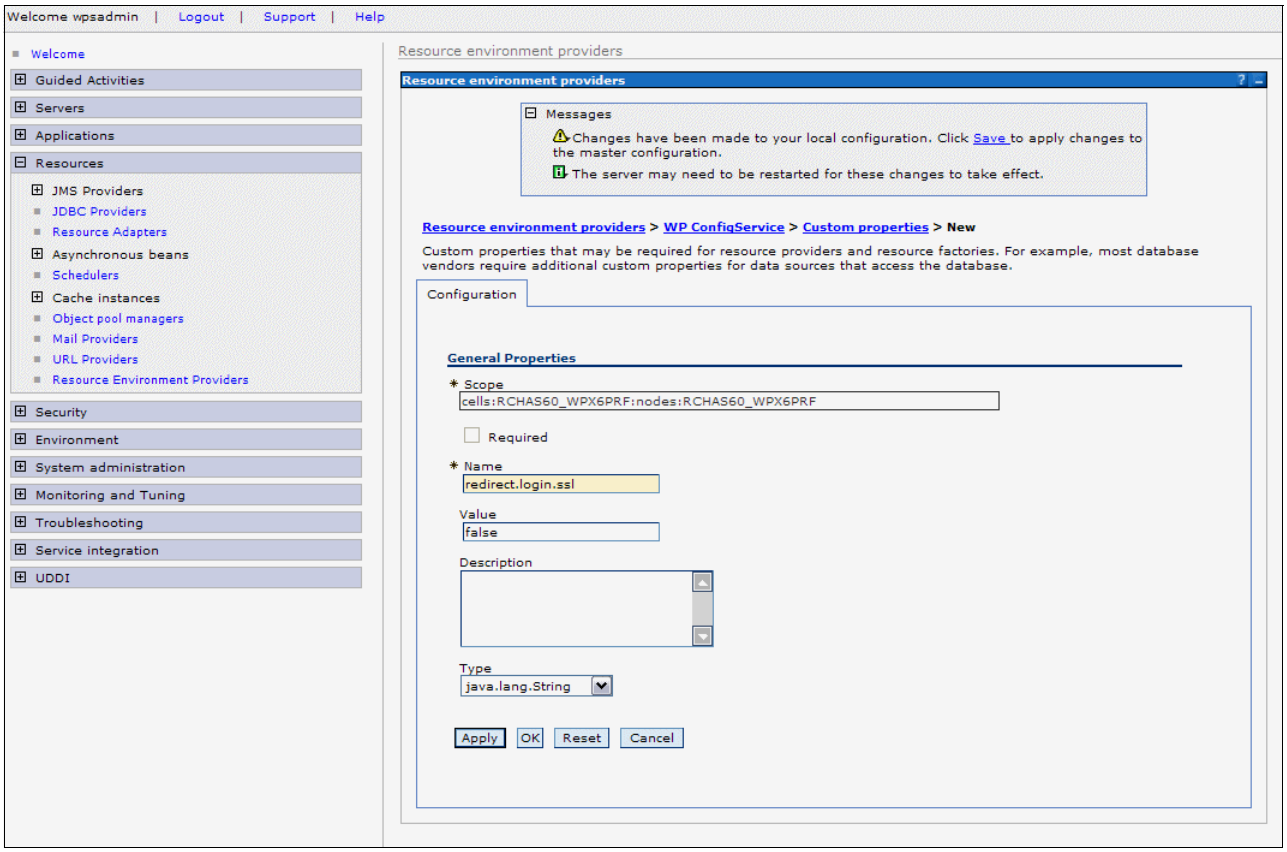


Figure 5-101 Custom property of redirect.login.ssl

7. Save the changes to the master configuration file.

8. The ConfigService custom properties looks like Figure 5-102

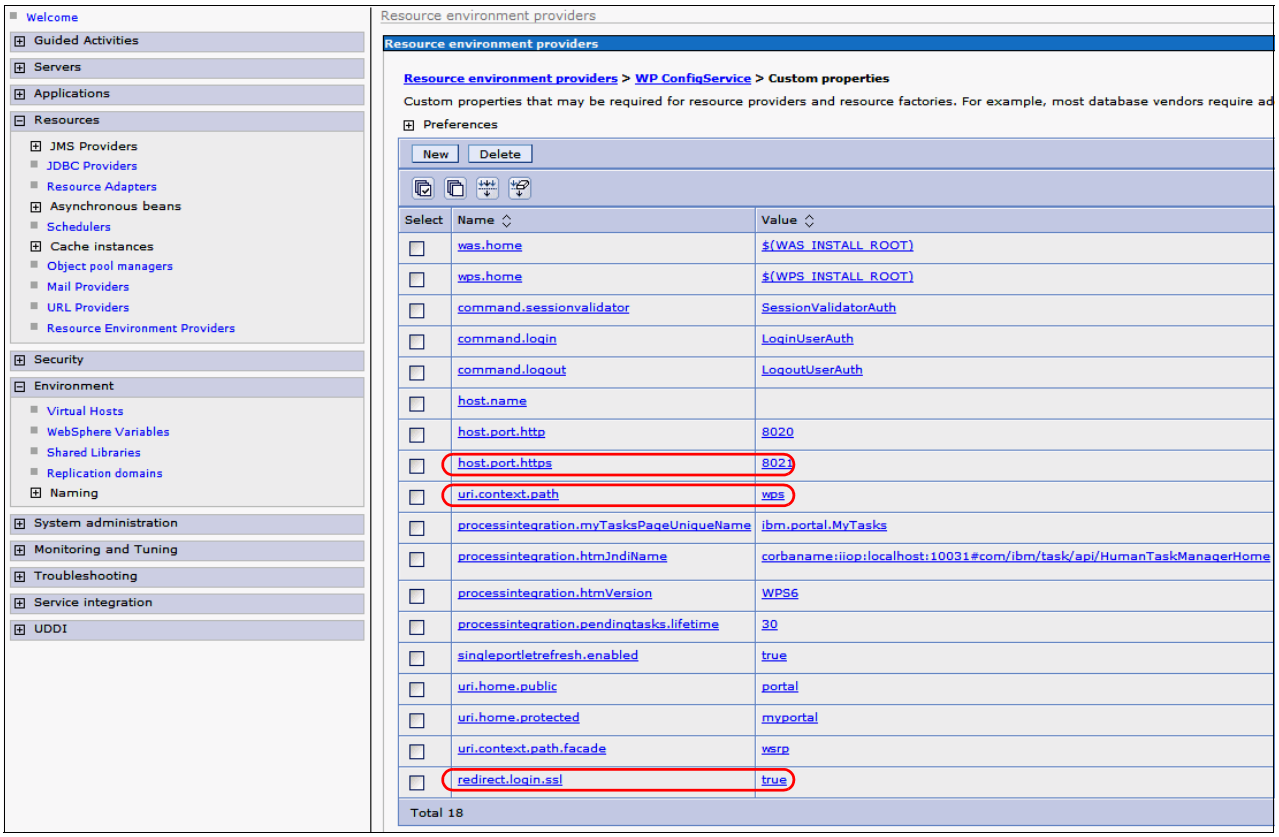


Figure 5-102 Portal service ConfigService configured for login encryption only

9. Exit the WebSphere Administration console.
10. Edit the file Web.xml located in the following i5/OS integrated file system directories:
   - /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/config/cells/*cell name*/applications/wps.ear/deployments/wps/wps.war/WEB-INF/Web.xml
   - /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/installedApps/*cellname*/wps.ear/wps.war/WEB-INF/Web.xml

For both files, check that the xml tag *<security-constraint id="SecurityConstraint_1">* contains the following xml tag *<transport-guarantee>NONE</transport-guarantee>*. Make sure that the value is set to `NONE`. See Figure 5-103.

```
<security-constraint id="SecurityConstraint_1">
      <web-resource-collection id="WebResourceCollection_1">
            <web-resource-name/>
            <url-pattern>/myportal/*</url-pattern>
            <http-method>DELETE</http-method>
            <http-method>GET</http-method>
            <http-method>POST</http-method>
            <http-method>PUT</http-method>
            <http-method>HEAD</http-method>
      </web-resource-collection>
      <auth-constraint id="AuthConstraint_1">
            <description/>
            <role-name>All Role</role-name>
      </auth-constraint>
      <user-data-constraint id="UserDataConstraint_4">
            <transport-guarantee>NONE</transport-guarantee>
      </user-data-constraint>
</security-constraint>
```

Figure 5-103 Portal application descriptor Web.xml

Note: If you need to make changes to this file, export and expand the wps.ear file. For information about updating and deploying the EAR file, see *Deploying themes and skins in a production environment* in the WebSphere Portal Express V6 Information Center at:

`http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/topic/com.ibm.wp.exp.doc/wps/dgn_dpycst.html#dgn_dpycst__deployprod`

11. Log in to WebSphere Portal Express as an administrator and select **Administration** → **Portlet Management** → **Portlets**, and search for the portlet with a title that starts with `Login`. See Figure 5-104**.**

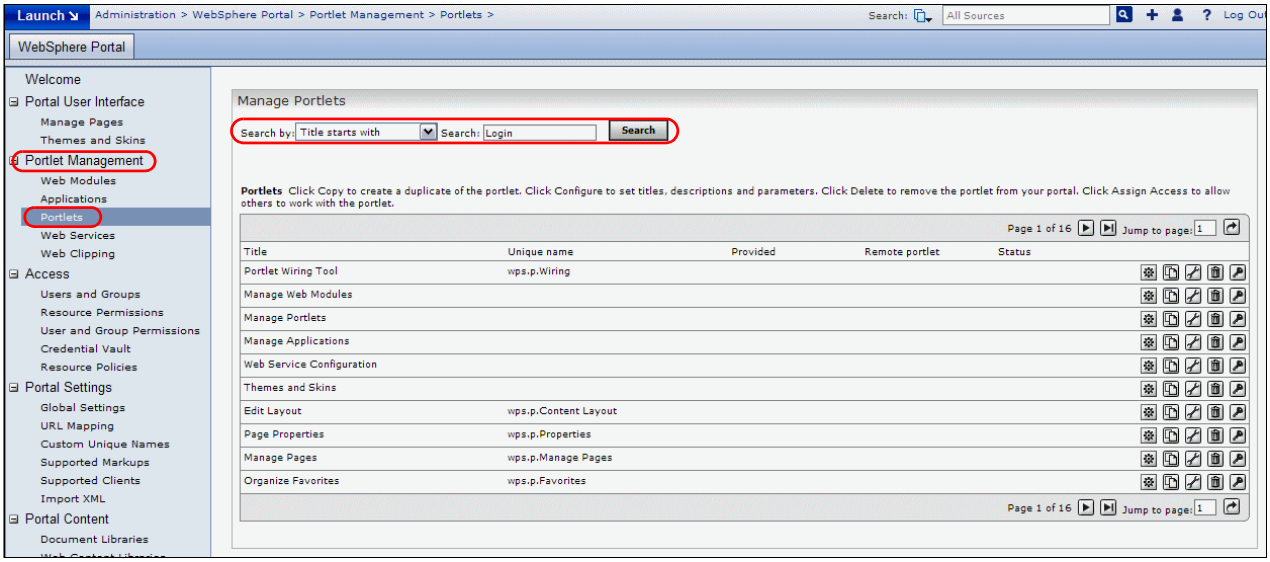


Figure 5-104 Portlet management

Note: If you are using the Login panel instead of the Login portlet, see the WebSphere Portal Express V6 Information Center at:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/topic/com.ibm.wp.exp.doc/wpf/config_ssl_login.html

12. Select the **Configure portlet** icon (Figure 5-105).

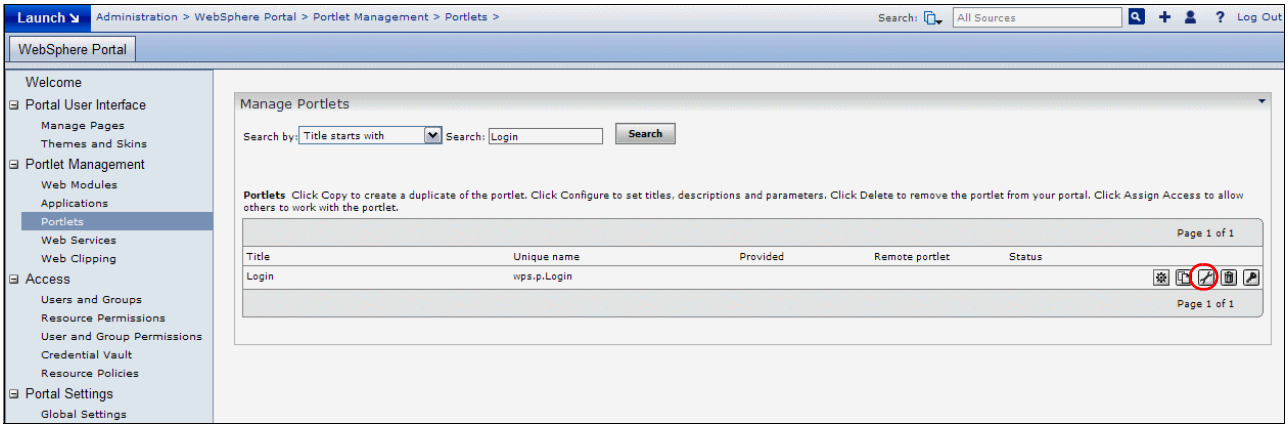


Figure 5-105 Configuring the login portlet

13. Edit the parameter UseSecureLoginActionUrl and set its value to **true**, then click **OK** (Figure 5-106).

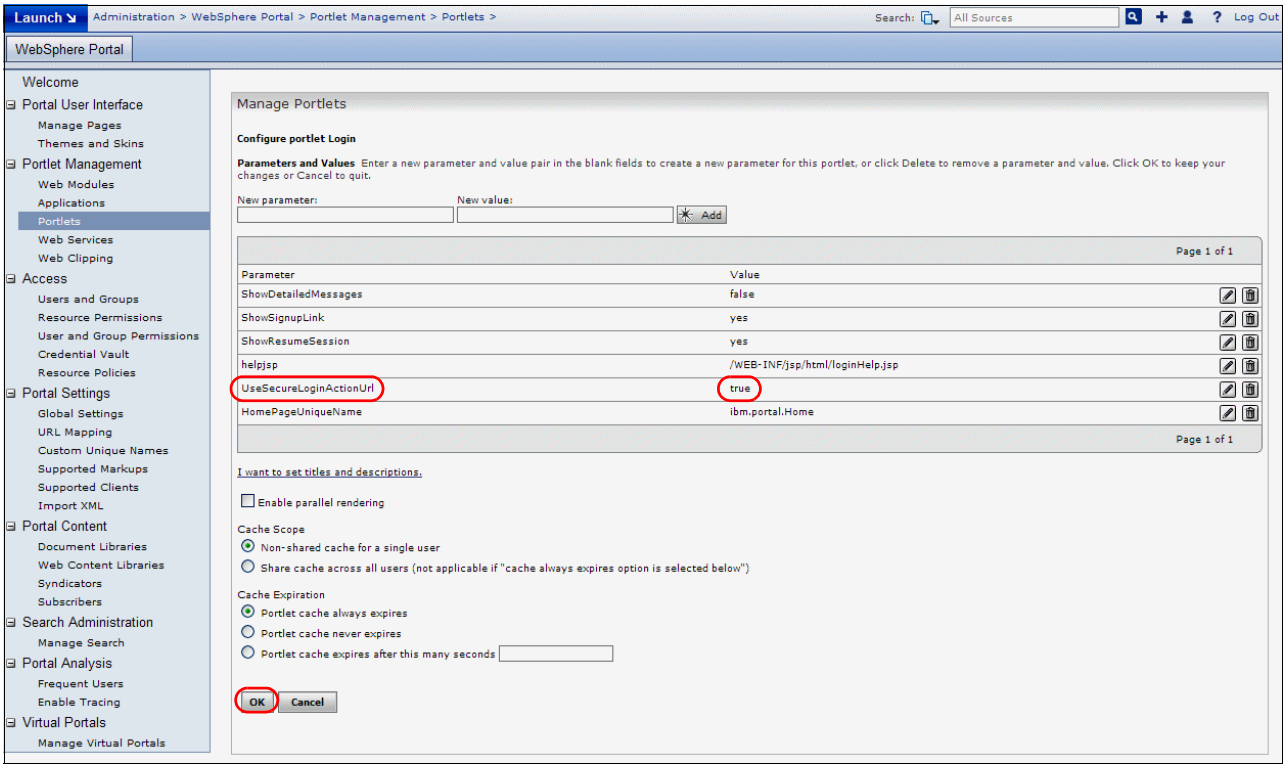


Figure 5-106 Setting the login portlet for secure login

14. Log out of WebSphere Portal Express.

15. Stop and restart your portal profile.

16. To check that your configuration is correct, access the portal login page and edit the source of this page (Figure 5-107).

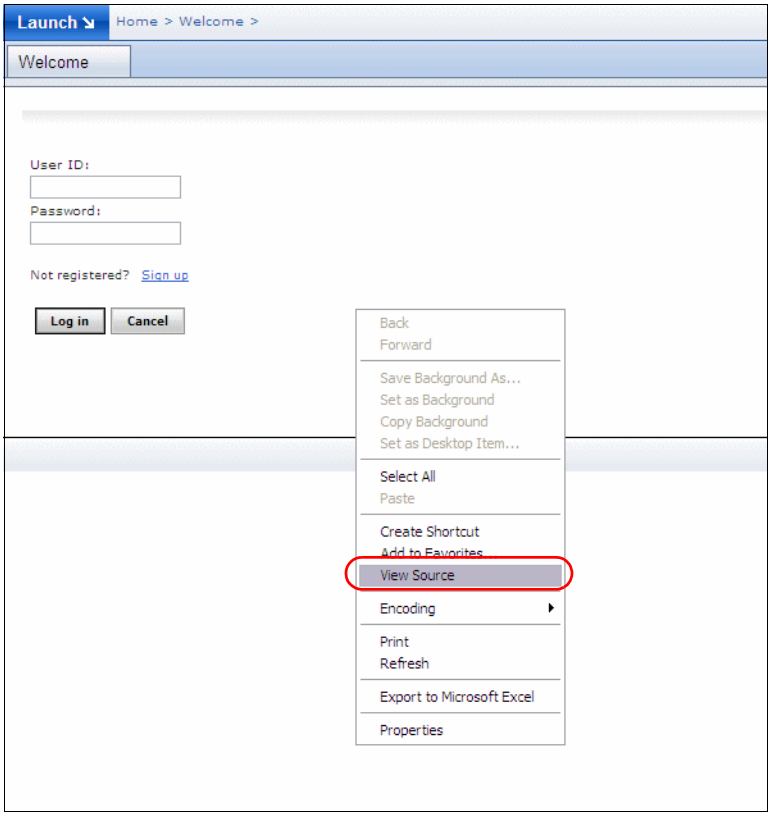


Figure 5-107 Accessing the portal login page source

17. The login form has an action URL that is secured. For example, *<form method="post" action="https://....">*. See Figure 5-108 and Figure 5-109.

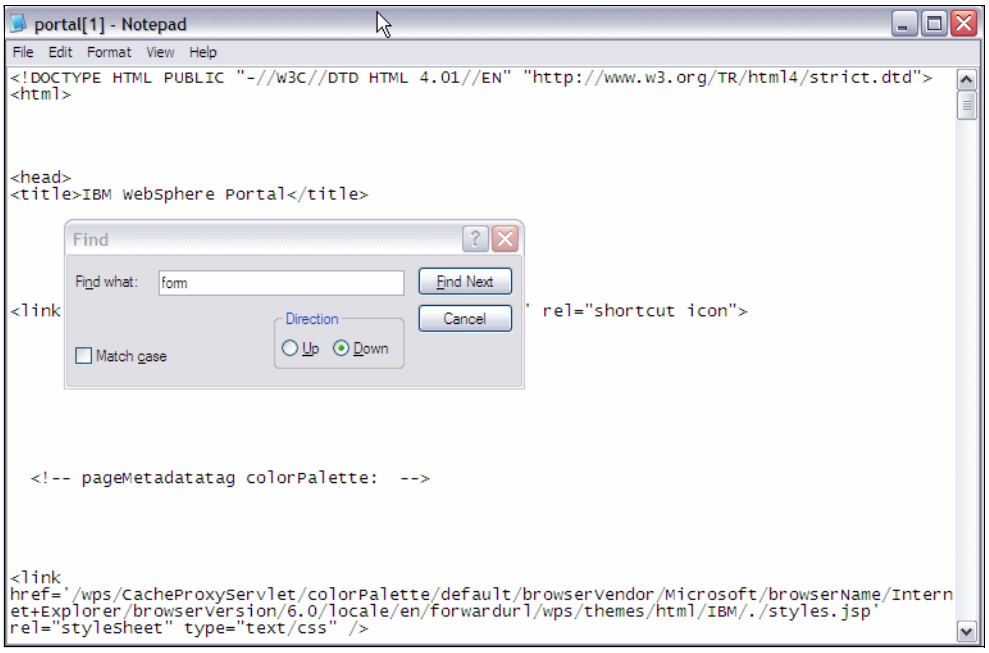


Figure 5-108 Checking the login configuration - Step 1

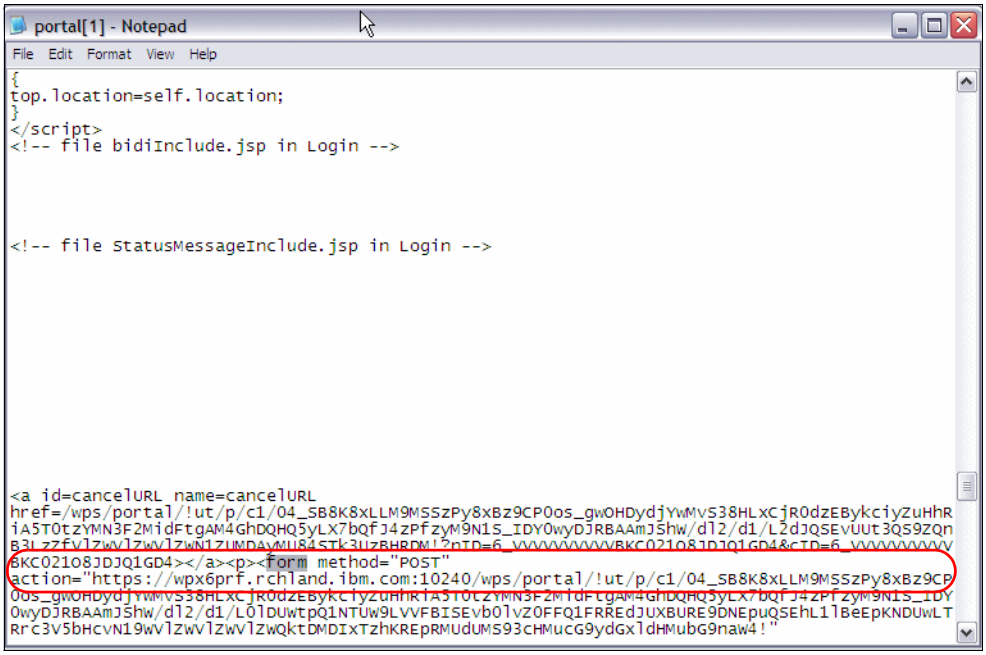


Figure 5-109 Checking the login configuration - Step 2

18. When clicking **Log in**, a pop-up window displays asking if you want to accept the Web site certificate (Figure 5-110). Another pop-up window warns that you are about to be redirected to an nonsecure connection (Figure 5-111).

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 5-110 WebSphere Portal Express certificate

Security Alert
You are about to be redirected to a connection that is not secure.
The information you are sending to the current site might be retransmitted to a nonsecure site. Do you wish to continue?
Yes
No

Figure 5-111 Secure log in to WebSphere Portal

19. Click **OK** to accept. You are then logged in to WebSphere Portal Express (Figure 5-112).

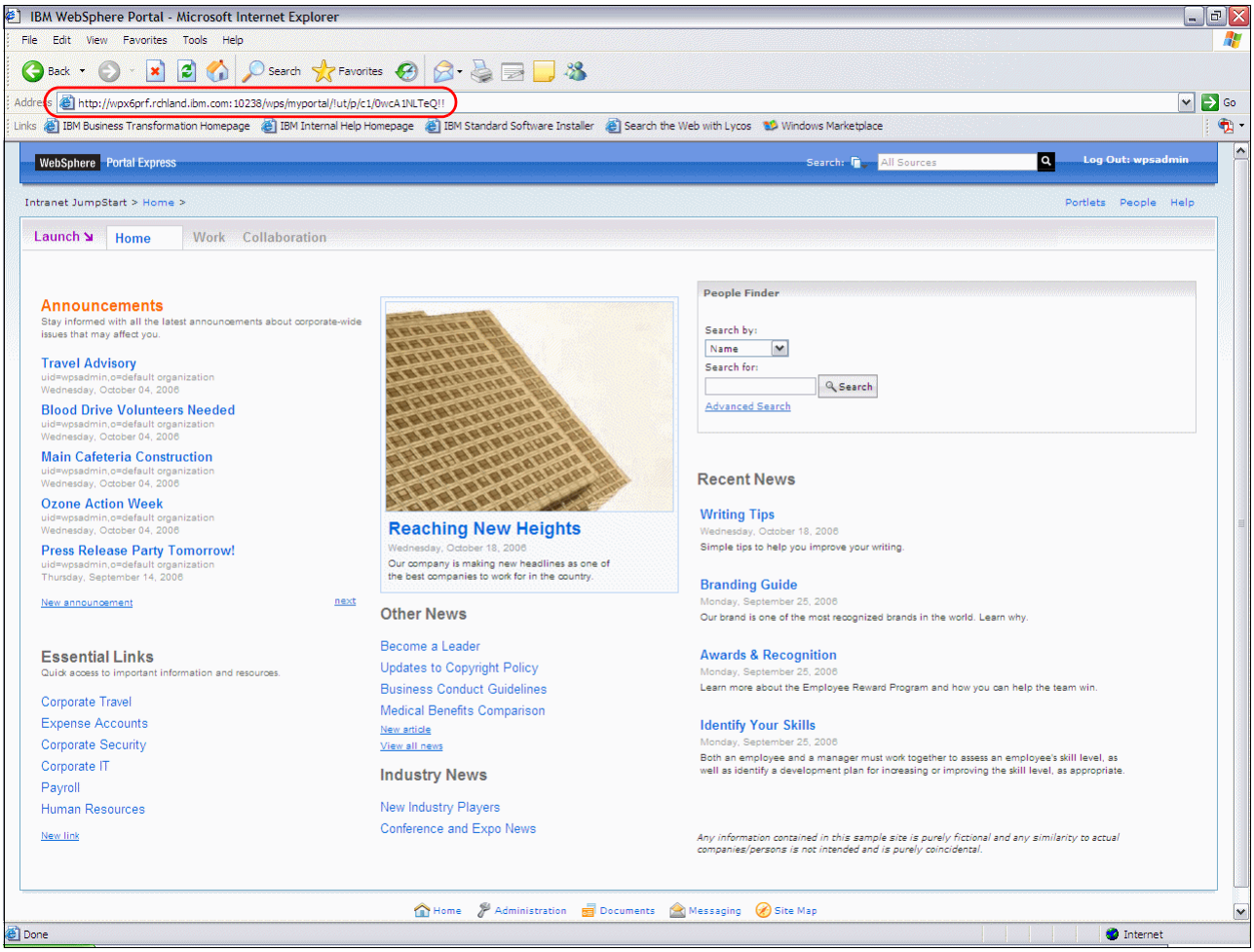

IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
http://wpx6prf.rchland.ibm.com:10238/wps/myportal/!ut/p/c1/0wcA1NLTeQ!!
IBM Business Transformation Homepage
IBM Internal Help Homepage
IBM Standard Software Installer
Search the Web with Lycos
Windows Marketplace
WebSphere Portal Express
Search: All Sources
Log Out: wpsadmin
Intranet JumpStart > Home >
Portlets People Help
Launch
Home
Work
Collaboration
Announcements
Stay informed with all the latest announcements about corporate-wide issues that may affect you.
Travel Advisory
Blood Drive Volunteers Needed
Main Cafeteria Construction
Ozone Action Week
Press Release Party Tomorrow!
New announcement
next
Essential Links
Quick access to important information and resources.
Corporate Travel
Expense Accounts
Corporate Security
Corporate IT
Payroll
Human Resources
New link
Reaching New Heights
Wednesday, October 18, 2006
Our company is making new headlines as one of the best companies to work for in the country.
Other News
Become a Leader
Updates to Copyright Policy
Business Conduct Guidelines
Medical Benefits Comparison
New article
View all news
Industry News
New Industry Players
Conference and Expo News
People Finder
Search by:
Name
Search for:
Search
Advanced Search
Recent News
Writing Tips
Simple tips to help you improve your writing.
Branding Guide
Our brand is one of the most recognized brands in the world. Learn why.
Awards & Recognition
Learn more about the Employee Reward Program and how you can help the team win.
Identify Your Skills
Both an employee and a manager must work together to assess an employee's skill level, as well as identify a development plan for increasing or improving the skill level, as appropriate.
Any information contained in this sample site is purely fictional and any similarity to actual companies/persons is not intended and is purely coincidental.
Home Administration Documents Messaging Site Map
Done
Internet

Figure 5-112 Secure log in process only

> **Note:** Check that the URL does not change to https when logging in.

The login process for your WebSphere Portal Express is now fully secured from end-to-end.

5.2.4 Enabling WebSphere Portal Express for SSL: All pages

This section describes the steps that are necessary to encrypt all the portal content. If you want to only secure the login process, refer to 5.2.3, “Enabling WebSphere Portal Express for SSL: login only” on page 217. Perform the following steps:

1. Configuring the portal service ConfigService:
   a. Open a Web browser and log in to the WebSphere Administration console.

b. In the left navigation pane, expand **Resources** and select **Resource Environment Provider**, then in the right pane of the browser, click **WP_ConfigService** (Figure 5-113).

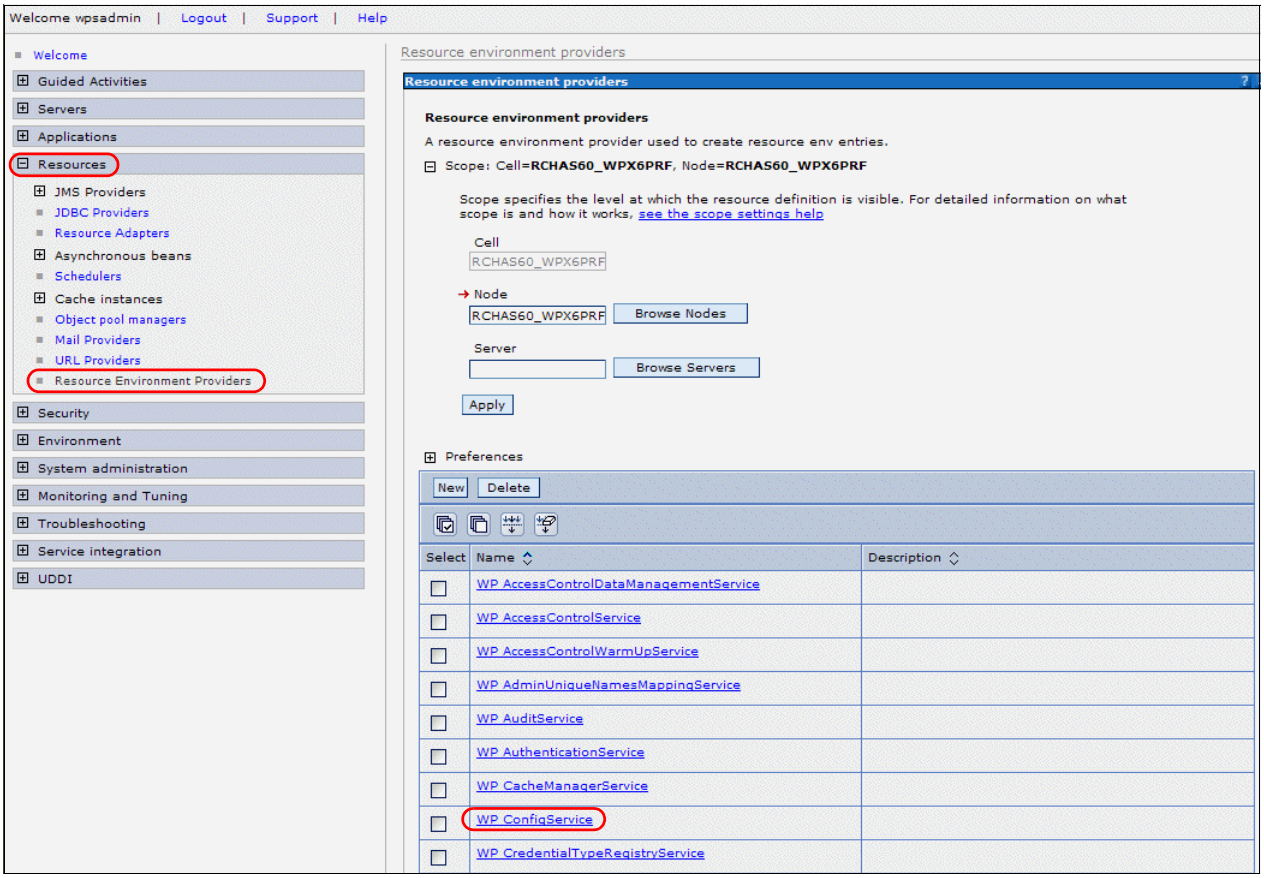


Figure 5-113 Accessing the portal service ConfigService

c. Click **Custom Properties** (Figure 5-114).

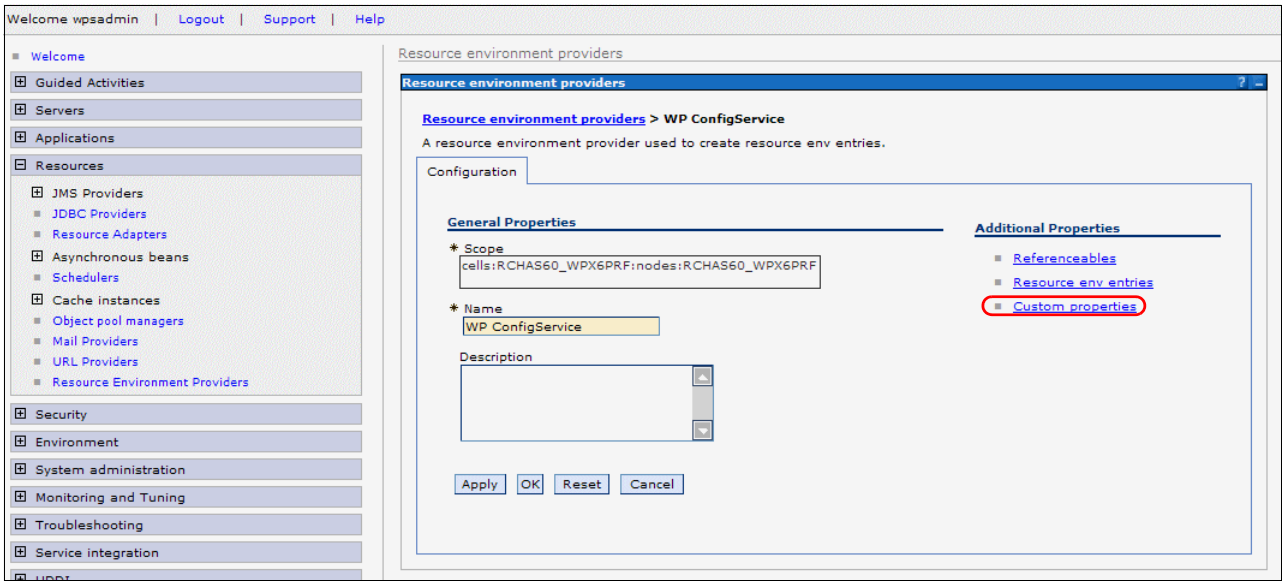


Figure 5-114 Portal service ConfigService custom properties

d. Set the custom property *host.port.http* to the value of the external HTTP Server nonsecure port (Figure 5-115).

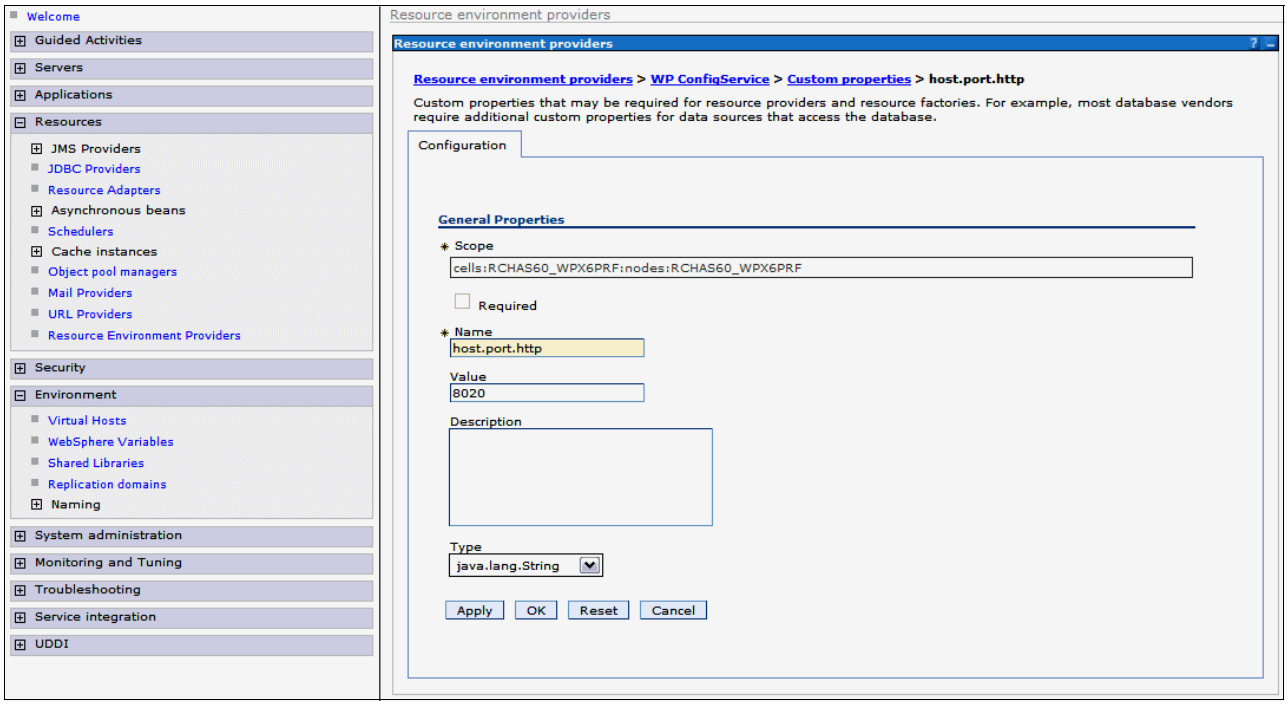


Figure 5-115 Custom property of host.port.http

e. Set the custom property *host.port.https* to the value of the external HTTP Server secure port (Figure 5-116).

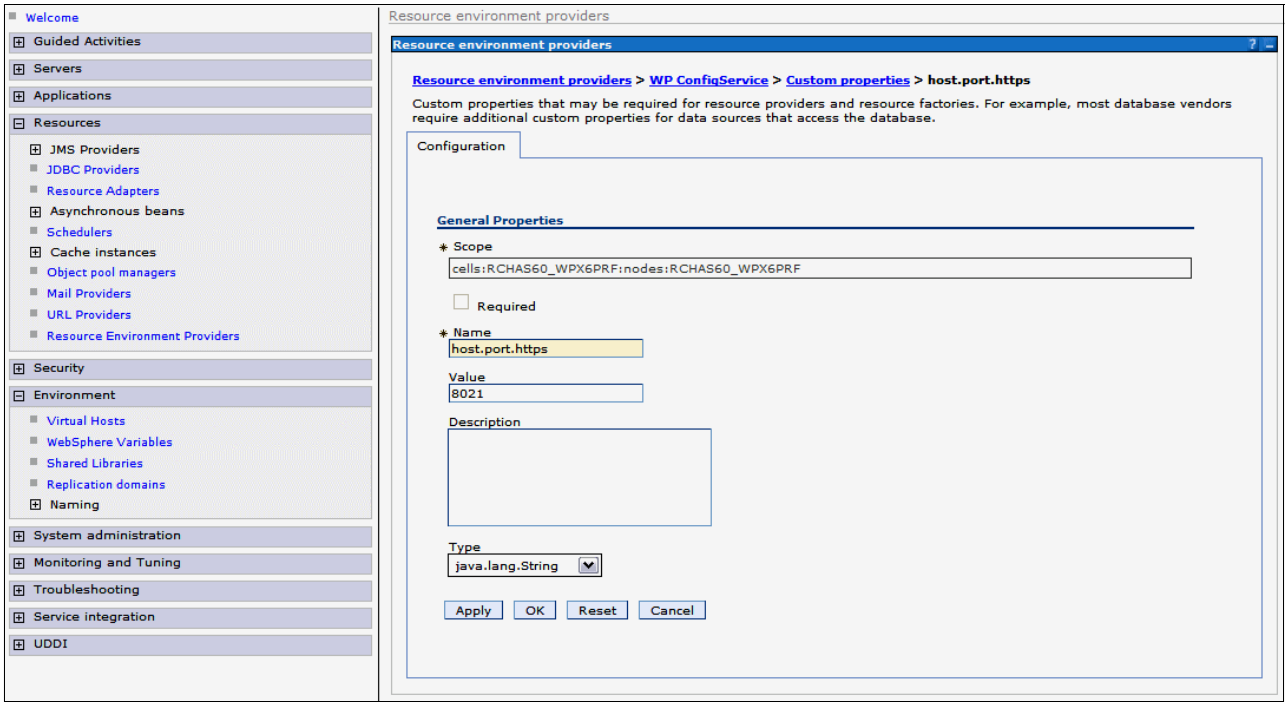


Figure 5-116 Custom property of host.port.https

f. Add the custom property *redirect.login.ssl* and set its value to *true* (Figure 5-117).

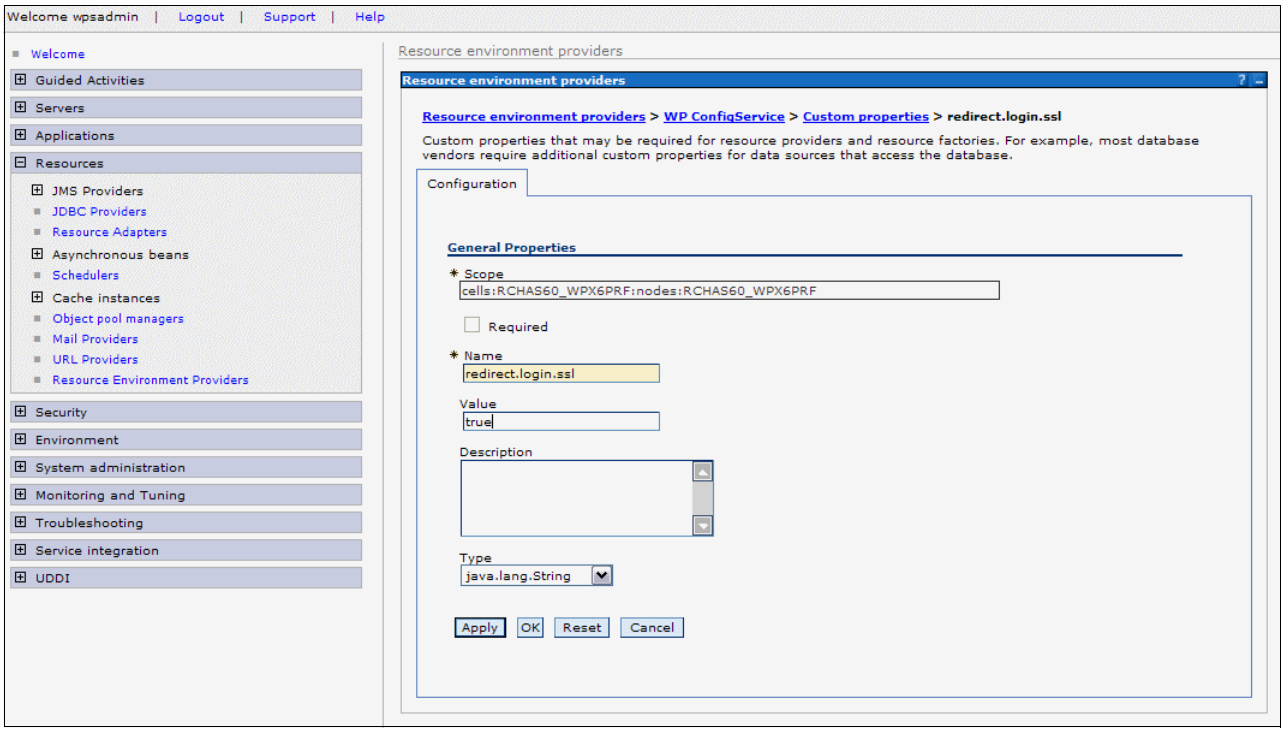


Figure 5-117 Custom property of redirect.login.ssl

g. Save the changes to the master configuration file.

h. The ConfigService custom properties looks like Figure 5-118.

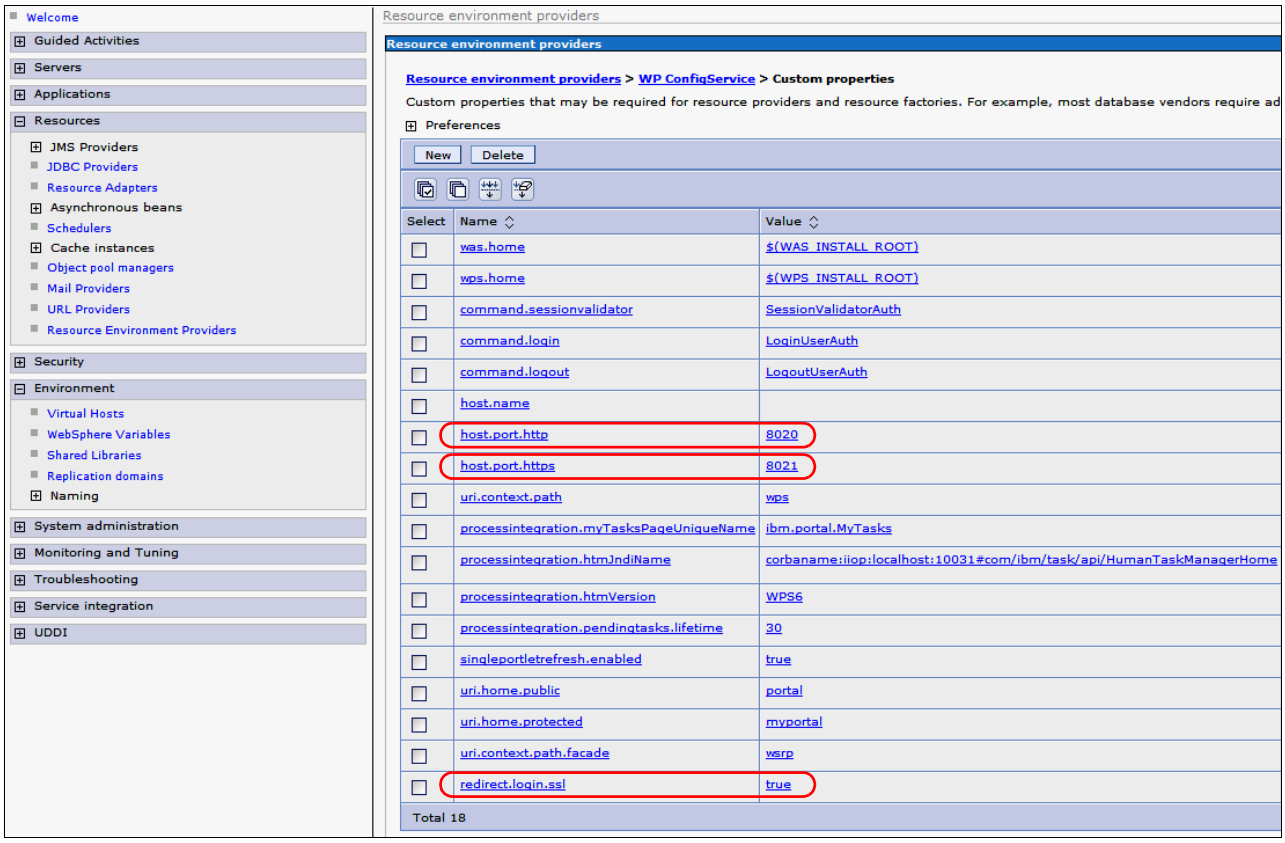


Figure 5-118 Portal service ConfigService configured for all portal content encryption

2. Perform the following steps to update the transport security constraints and themes:
   a. Open a Web browser and log in to the WebSphere Administration console.

b. In the left navigation pane, expand **Applications** and select **Enterprise Applications**, and then in the right pane, page down the application list until you see the application wps, usually on the last page (Figure 5-119).

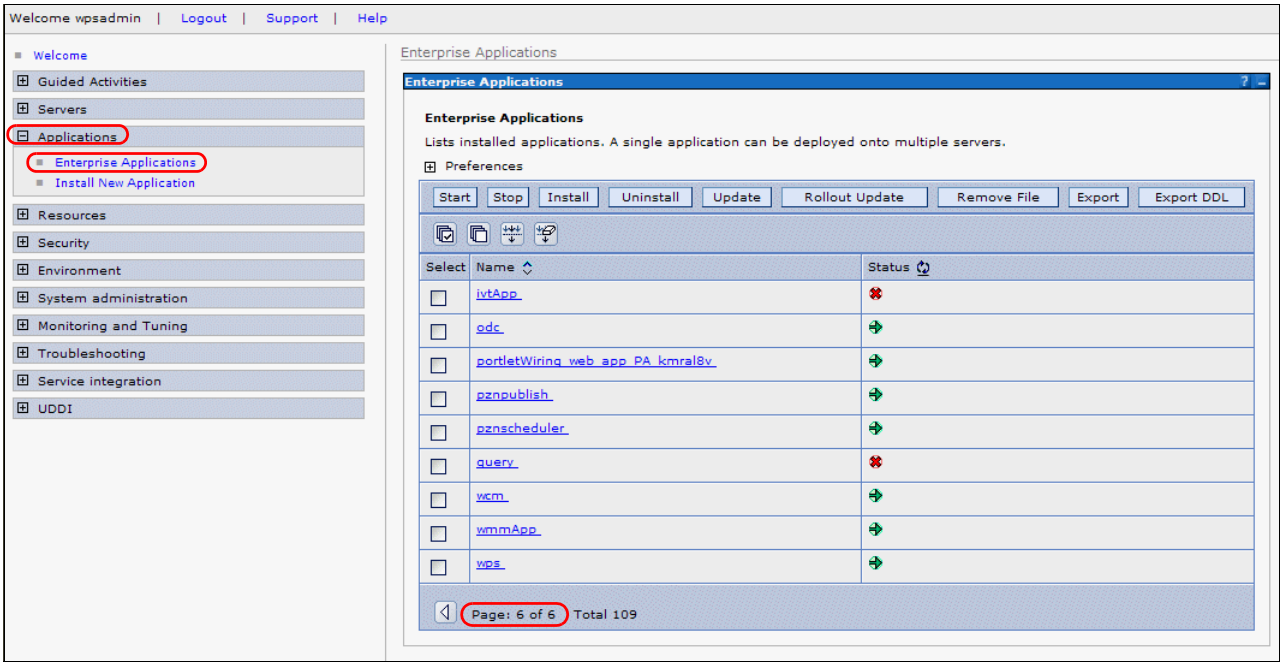


Figure 5-119 Accessing wps application

c. Check the check box for **wps** and click **Export** (Figure 5-120).

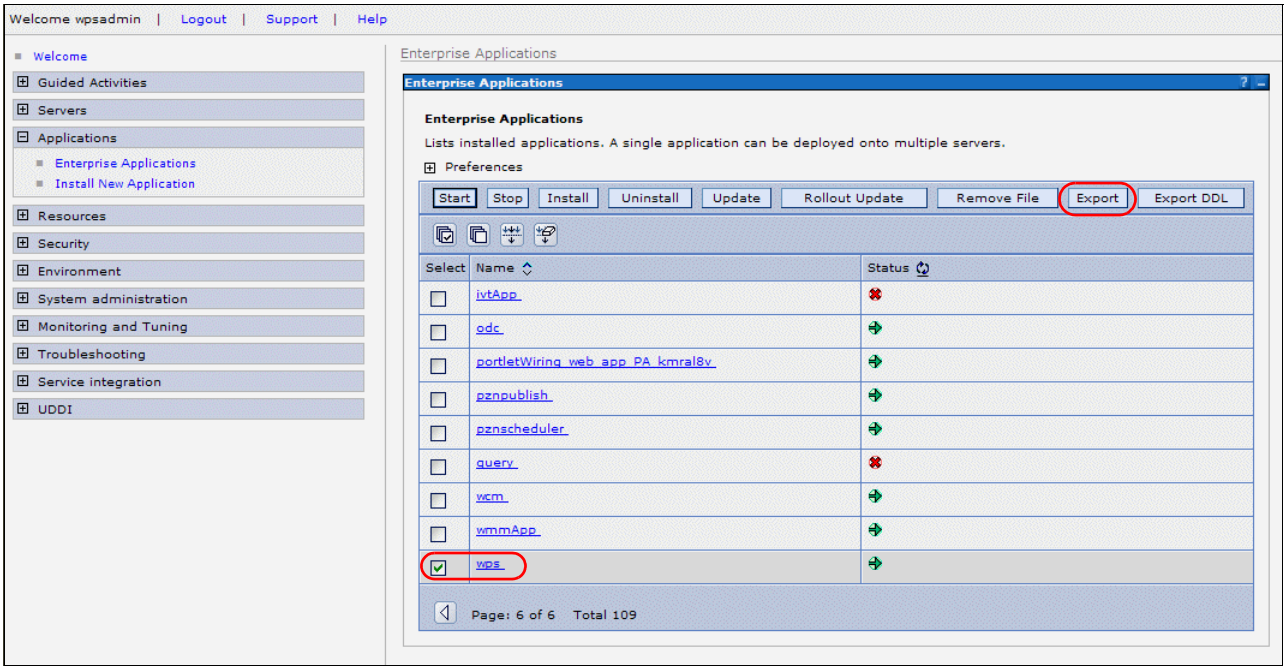


Figure 5-120 Managing wps application

d. Click **wps.ear** (Figure 5-121).

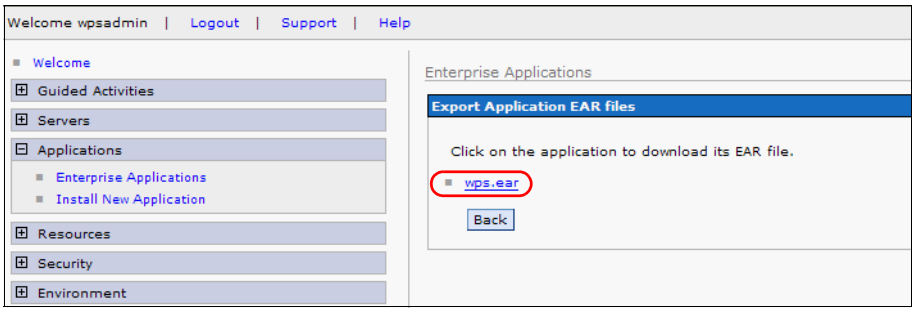


Figure 5-121 Exporting wps application

e. A pop-up window is displayed asking if you want to save this file. Click **Save** (Figure 5-122).

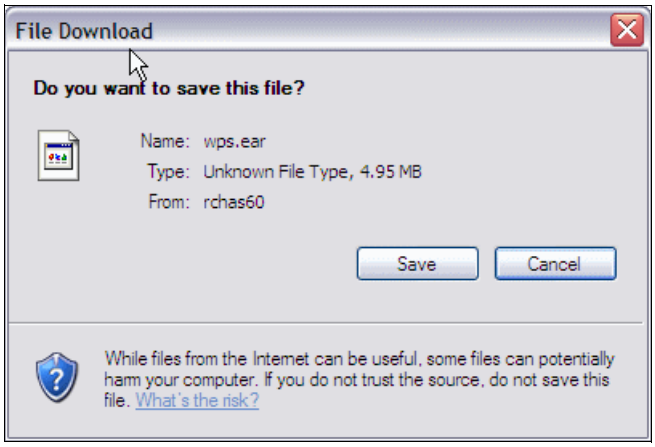

File Download
Do you want to save this file?
Name: wps.ear
Type: Unknown File Type, 4.95 MB
From: rchas60
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

Figure 5-122 Saving the ear file

f. Save the file in the i5/OS integrated file system in a location of your choice.

g. From the directory where you exported the ear file, create a subfolder called `/wps_expanded`.

h. From a 5250 emulation session, enter the i5/OS CL command of Start Qshell (STRQSH).

i. Navigate to the i5/OS integrated file system directory of /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/*portal_profile*/bin.

j. From the Qshell session, expand the exported ear file using the following EARExpander command:

```
EARExpander -ear directory/wps.ear -operationDir directory/wps_expanded
-operation expand
```

Where *directory* is the directory path where you exported the ear file.

k. Delete the *wps.ear* file from the temporary directory.

l. Edit the Web.xml file in the directory *directory*/wps_expanded/wps.war/WEB-INF/Web.xml. Find the xml tag <security-constraint id="SecurityConstraint_1">. Within that tag, modify the xml tag

<transport-guarantee> value from `NONE` to `CONFIDENTIAL` (Figure 5-123). Save the file and close it.

```
<security-constraint id="SecurityConstraint_1">
      <web-resource-collection id="WebResourceCollection_1">
            <web-resource-name/>
            <url-pattern>/myportal/*</url-pattern>
            <http-method>DELETE</http-method>
            <http-method>GET</http-method>
            <http-method>POST</http-method>
            <http-method>PUT</http-method>
            <http-method>HEAD</http-method>
      </web-resource-collection>
      <auth-constraint id="AuthConstraint_1">
            <description/>
            <role-name>All Role</role-name>
      </auth-constraint>
      <user-data-constraint id="UserDataConstraint_4">
            <transport-guarantee>CONFIDENTIAL</transport-guarantee>
      </user-data-constraint>
</security-constraint>
```

Figure 5-123 Updating the security constraint

m. In the directory *directory*/wps_expanded/wps.war/themes, search for all JSP™ and JSPF files containing the string wps.Login. First, map a network drive to the i5/OS integrated file system, and then perform the search from a DOS prompt using the following command:

```
findstr /s /m wps.Login *.*
```

Figure 5-124 shows the result for our portal profile.

```
Y:\home\pguerton\wps_expanded\wps.war\themes>findstr /s /m wps.Login *.*
html\Default.jsp
html\Express\banner_toolbar.jspf
html\Express\mainMenu.jsp
html\IBM\banner_toolbar.jspf
html\IBM\mainMenu.jsp

Y:\home\pguerton\wps_expanded\wps.war\themes>
```

Figure 5-124 Searching for wps.Login in the portal themes

n. For each file containing the string *wps.Login*, find the tag *<portal-navigation:urlGeneration* and add the `ssl="true"` attribute to this tag (Figure 5-125). Save the file.

```
<portal-navigation:urlGeneration contentNode="wps.Login" ssl="true">
          <a tabIndex="7" class="toolbarLink" href='<% wpsURL.write(escapeXmlWriter); %>'>
          <portal-fmt:text key="link.login" bundle="nls.engine"/>
          </a>
 </portal-navigation:urlGeneration>
```

Figure 5-125 Updating the portal themes for SSL

Note: The tag prefix *portal-navigation* might be different, depending on which tag library is used.

o. From the Qshell session, collapse the expanded ear file using the following EARExpander command:

```
EARExpander -ear directory/wps.ear -operationDir directory/wps_expanded
-operation collapse
```

Where *directory* is the directory path where you exported the ear file.

p. Update the wps application from the WebSphere Administration Console. Expand **Applications** and select **Enterprise Applications**. Then page down the application list until you see the application wps.

q. Check the check box for **wps** and click **Update** (Figure 5-126).

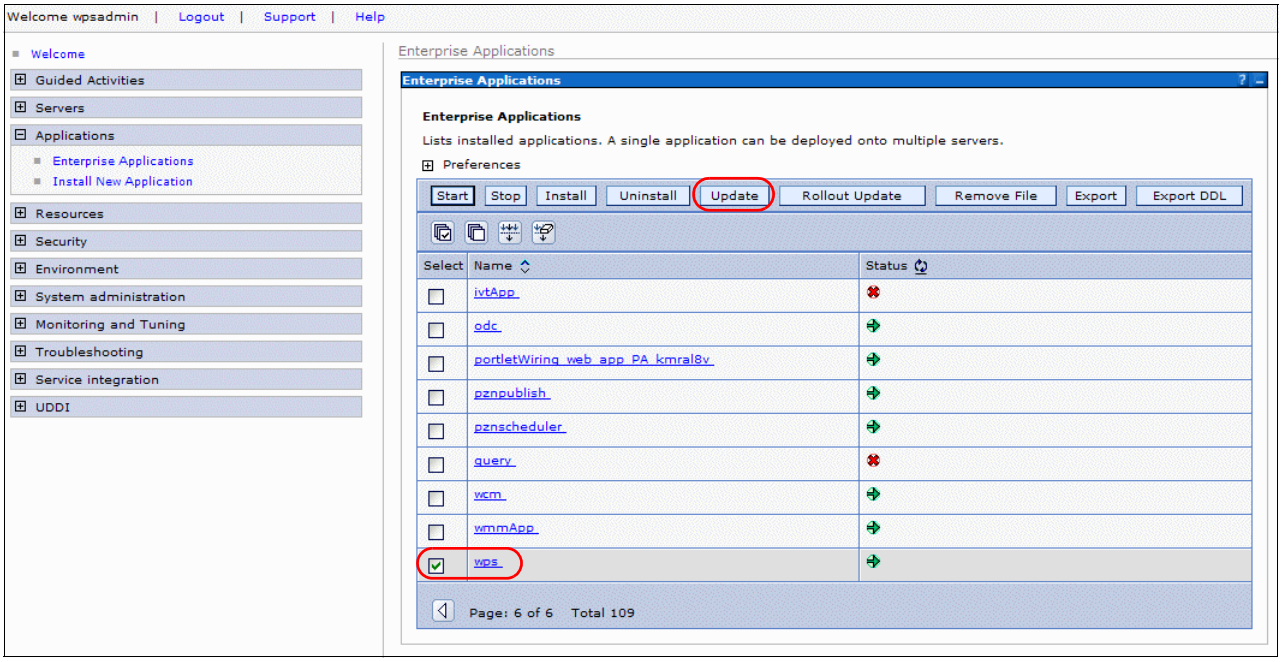


Figure 5-126 Managing the wps application

r. Click the radio button **Full application**, then the radio button **Local file system** and specify the path of the collapsed ear file. Click **Next** (Figure 5-127).

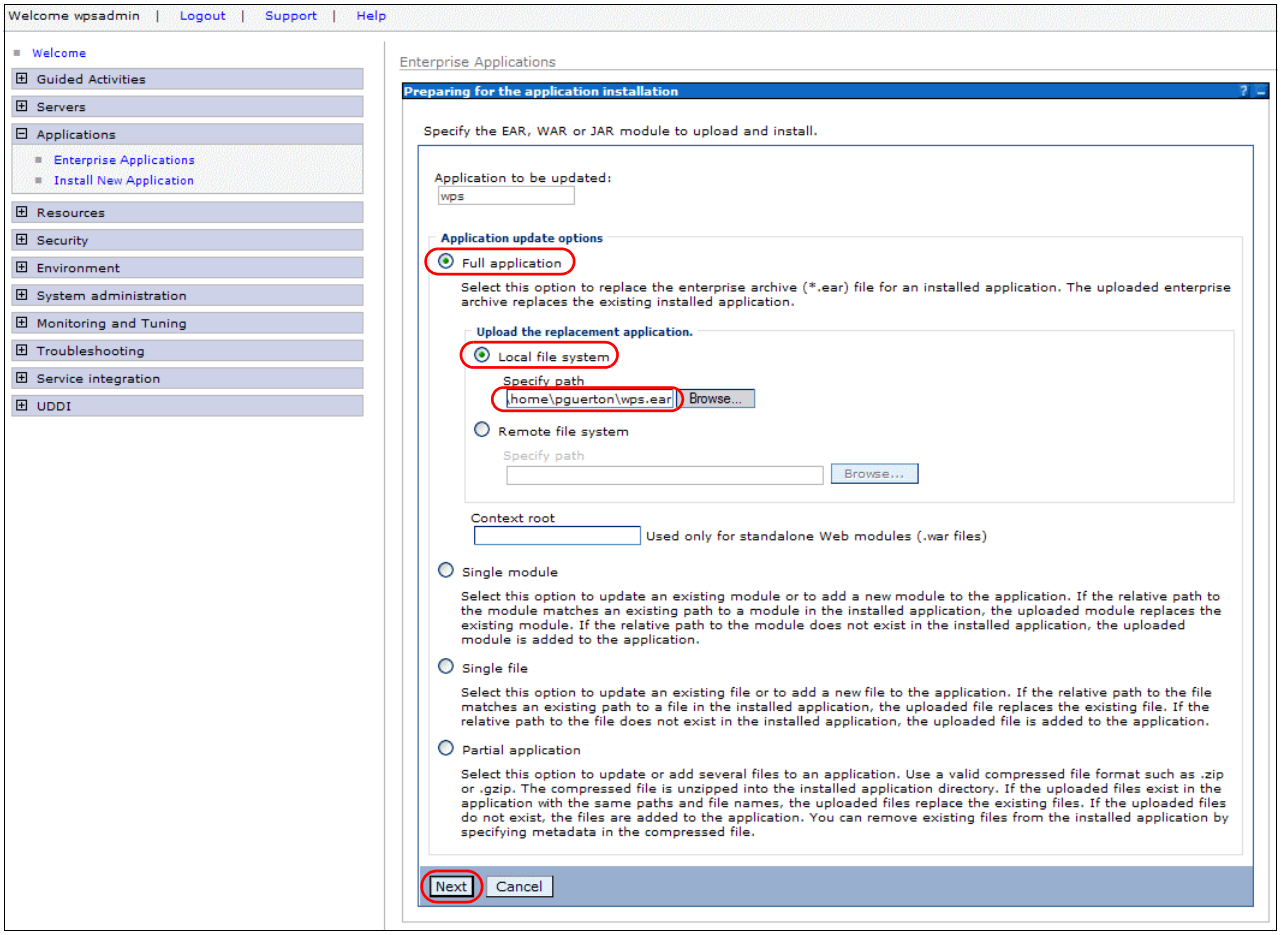

Welcome wpsadmin | Logout | Support | Help
Welcome
Guided Activities
Servers
Applications
Enterprise Applications
Install New Application
Resources
Security
Environment
System administration
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Enterprise Applications
Preparing for the application installation
Specify the EAR, WAR or JAR module to upload and install.
Application to be updated:
wps
Application update options
Full application
Select this option to replace the enterprise archive (*.ear) file for an installed application. The uploaded enterprise archive replaces the existing installed application.
Upload the replacement application.
Local file system
Specify path
home\pguerton\wps.ear
Browse...
Remote file system
Specify path
Browse...
Context root
Used only for standalone Web modules (.war files)
Single module
Select this option to update an existing module or to add a new module to the application. If the relative path to the module matches an existing path to a module in the installed application, the uploaded module replaces the existing module. If the relative path to the module does not exist in the installed application, the uploaded module is added to the application.
Single file
Select this option to update an existing file or to add a new file to the application. If the relative path to the file matches an existing path to a file in the installed application, the uploaded file replaces the existing file. If the relative path to the file does not exist in the installed application, the uploaded file is added to the application.
Partial application
Select this option to update or add several files to an application. Use a valid compressed file format such as .zip or .gzip. The compressed file is unzipped into the installed application directory. If the uploaded files exist in the application with the same paths and file names, the uploaded files replace the existing files. If the uploaded files do not exist, the files are added to the application. You can remove existing files from the installed application by specifying metadata in the compressed file.
Next
Cancel

Figure 5-127 Specifying the ear file path

s. On the following windows, accept all the default values and click either **Next** or **Continue** until the last window where you click **Finish** (Figure 5-128).

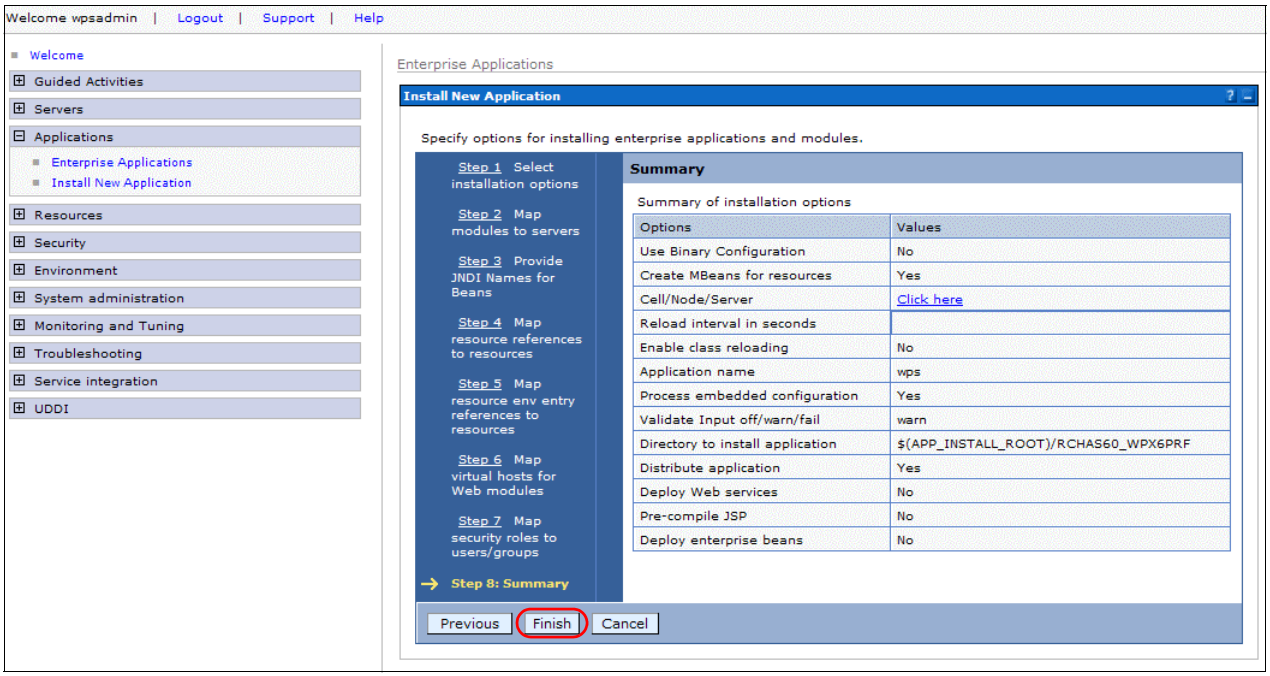


Figure 5-128 Updating the wps application

t. When the update is complete, save the changes to the master configuration file.

u. Exit the WebSphere Administration Console.

3. Enable the login portlet for SSL. See Steps 11 to 13 of 5.2.3, “Enabling WebSphere Portal Express for SSL: login only” on page 217.

4. Stop and restart the portal profile for the changes to take effect.

5. Test your changes:

a. Open a Web browser and access the portal home page (`http://wpx6prf.rchland.ibm.com:8020/wps/portal` in our example).

b. Check that the login link uses the HTTPS protocol (Figure 5-129).

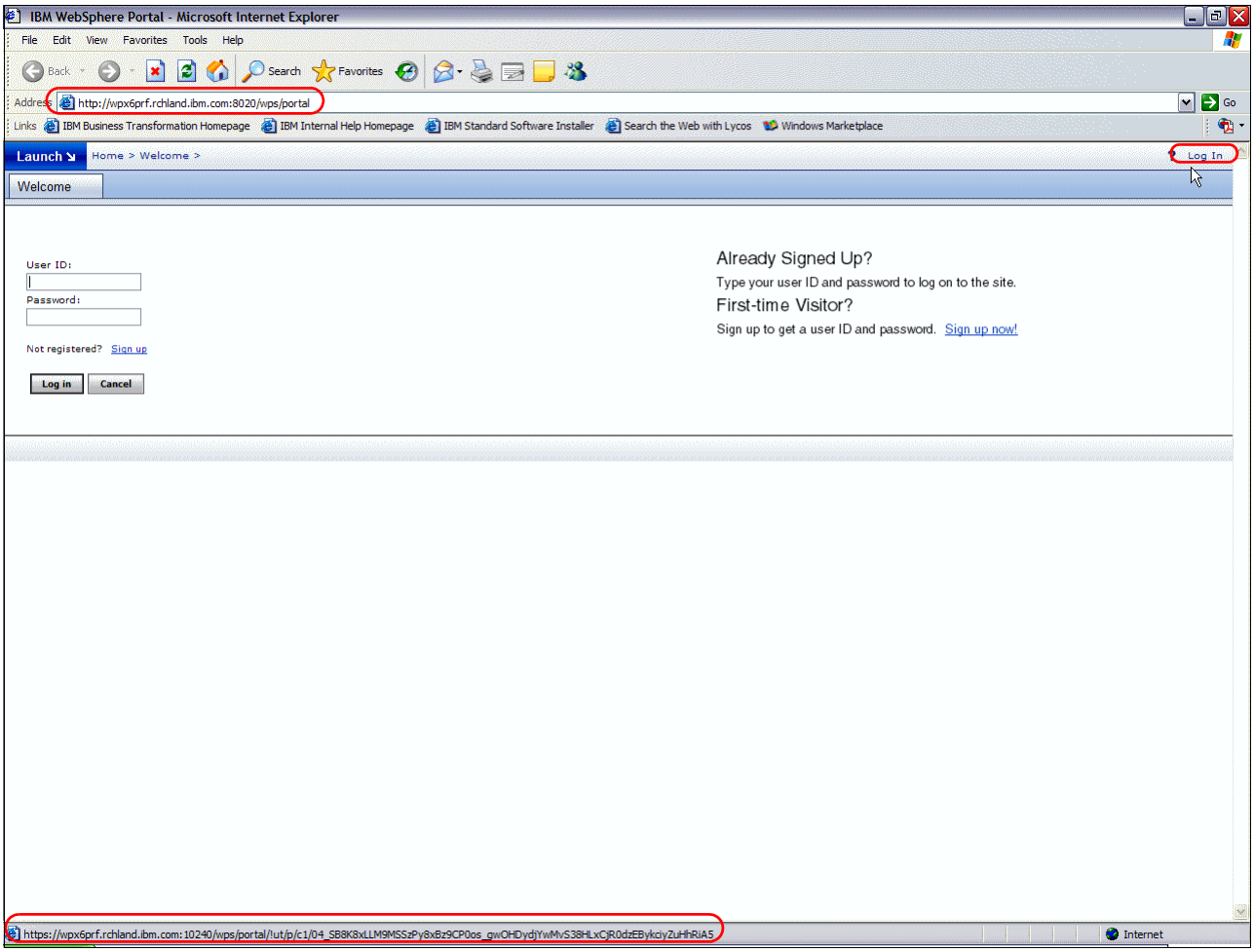

IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://wpx6prf.rchland.ibm.com:8020/wps/portal
Go
Links IBM Business Transformation Homepage IBM Internal Help Homepage IBM Standard Software Installer Search the Web with Lycos Windows Marketplace
Launch
Home > Welcome >
Log In
Welcome
User ID:
Password:
Not registered? Sign up
Log in
Cancel
Already Signed Up?
Type your user ID and password to log on to the site.
First-time Visitor?
Sign up to get a user ID and password. Sign up now!
https://wpx6prf.rchland.ibm.com:10240/wps/portal/!ut/p/c1/04_SB8K8xLLM9MSSzPy8xBz9CP0os_gwOHDydjYwMvS38HLxCjR0dzEBykciyZuHnRiA5
Internet

Figure 5-129 Testing the public portal home page

c. Click that link and check that you are asked to accept the Web server certificate. Click **Yes** to accept it (Figure 5-130).

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 5-130 Accepting the certificate

d. You are then redirected to the login page. Check that this page is encrypted (Figure 5-131).

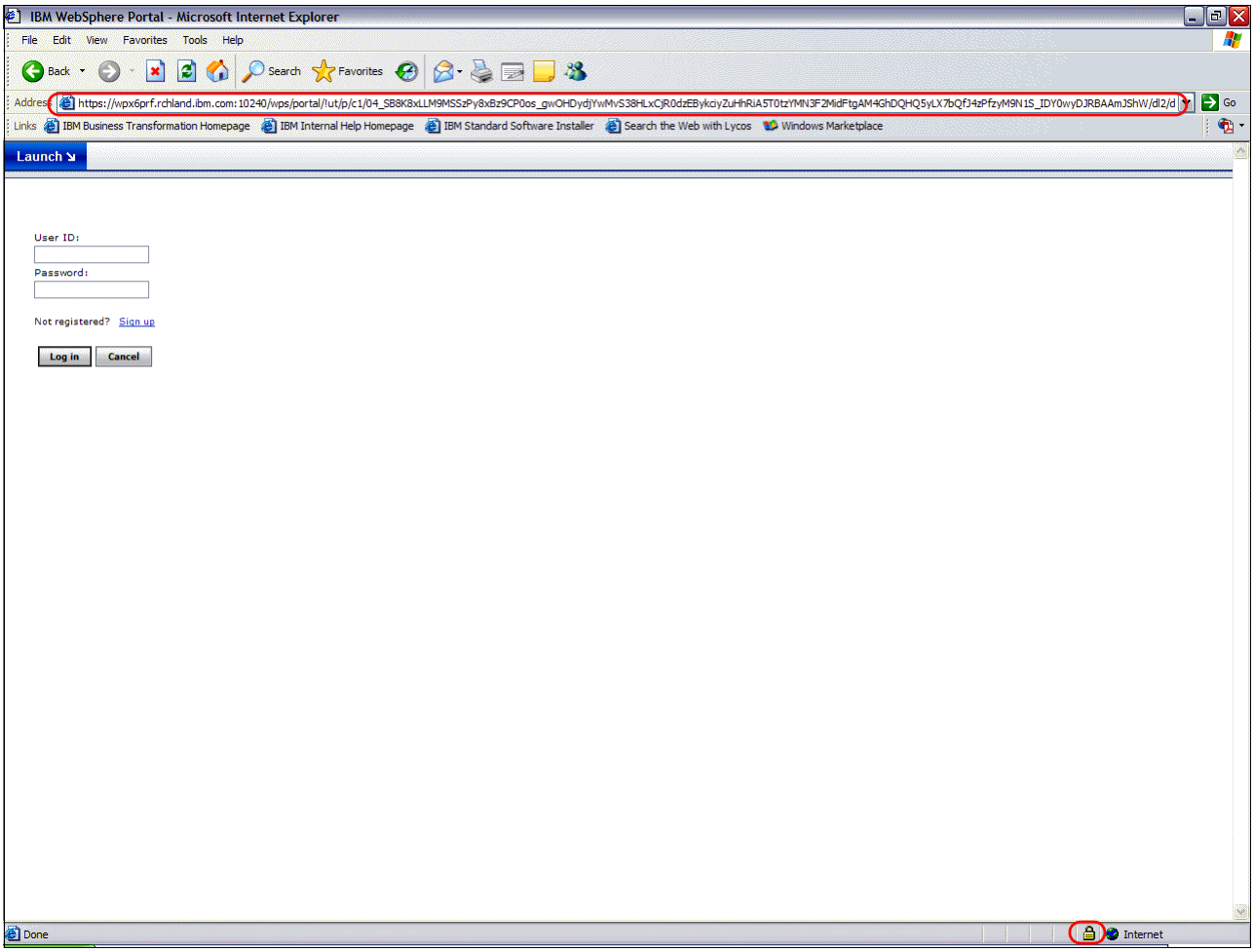


Figure 5-131 Encrypted portal login page

e. Log in to the portal and check that the home page is encrypted (Figure 5-132).

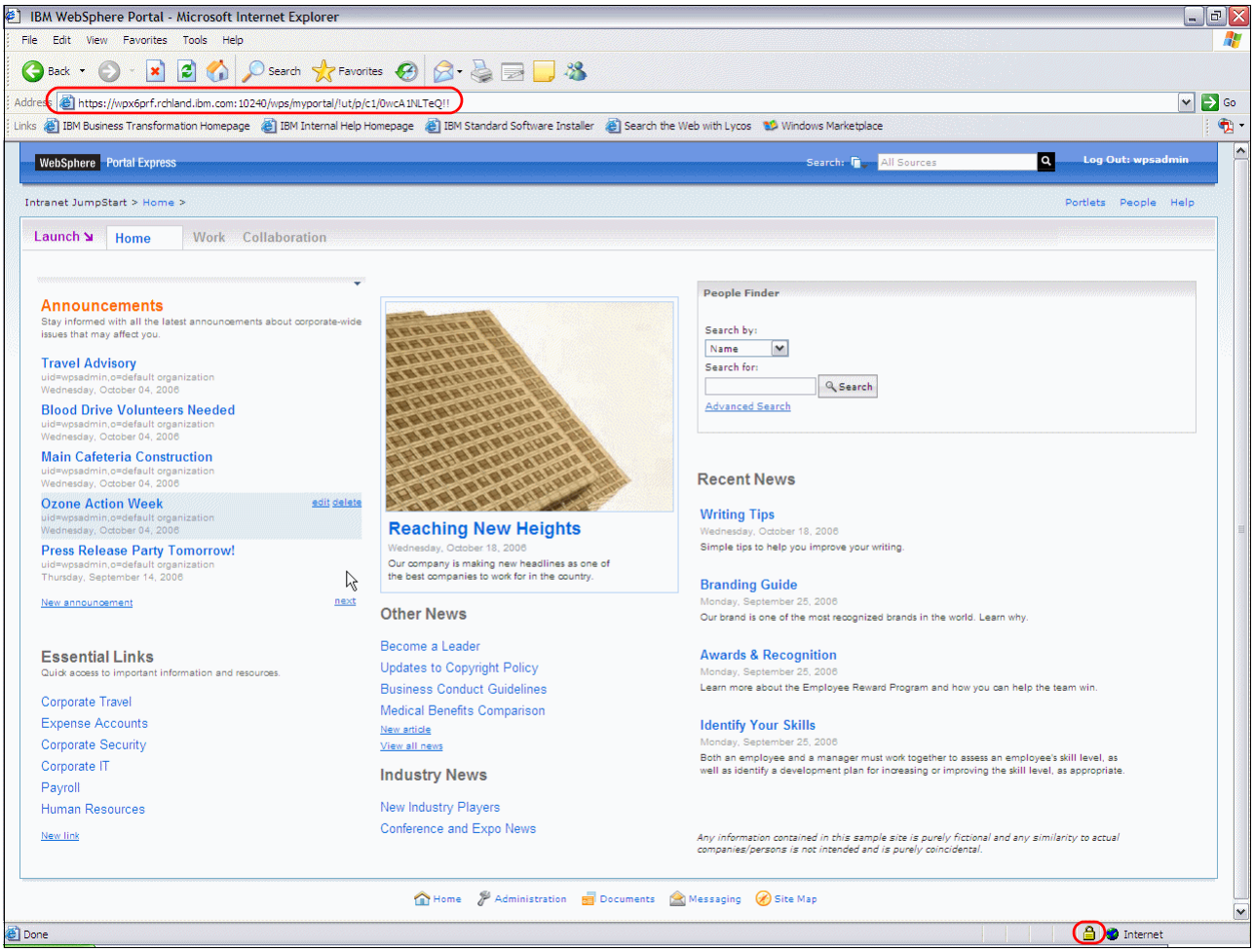

IBM WebSphere Portal - Microsoft Internet Explorer
https://wpx6prf.rchland.ibm.com:10240/wps/myportal/!ut/p/c1/0wcA1NLTeQ!!
WebSphere Portal Express
Log Out: wpsadmin
Intranet JumpStart > Home >
Portlets People Help
Launch Home Work Collaboration
Announcements
Stay informed with all the latest announcements about corporate-wide issues that may affect you.
Travel Advisory
Blood Drive Volunteers Needed
Main Cafeteria Construction
Ozone Action Week
Press Release Party Tomorrow!
New announcement
next
Essential Links
Quick access to important information and resources.
Corporate Travel
Expense Accounts
Corporate Security
Corporate IT
Payroll
Human Resources
New link
Reaching New Heights
Wednesday, October 18, 2006
Our company is making new headlines as one of the best companies to work for in the country.
Other News
Become a Leader
Updates to Copyright Policy
Business Conduct Guidelines
Medical Benefits Comparison
New article
View all news
Industry News
New Industry Players
Conference and Expo News
People Finder
Search by:
Name
Search for:
Search
Advanced Search
Recent News
Writing Tips
Simple tips to help you improve your writing.
Branding Guide
Our brand is one of the most recognized brands in the world. Learn why.
Awards & Recognition
Learn more about the Employee Reward Program and how you can help the team win.
Identify Your Skills
Both an employee and a manager must work together to assess an employee's skill level, as well as identify a development plan for increasing or improving the skill level, as appropriate.
Any information contained in this sample site is purely fictional and any similarity to actual companies/persons is not intended and is purely coincidental.
Home Administration Documents Messaging Site Map
Done
Internet

Figure 5-132 Encrypted portal home page

Your WebSphere Portal Express profile is now configured to secure all content, including the login process.

6

Online backup and recovery

This chapter describes how to save an IBM WebSphere Portal Express V6 profile while it is online and in active use. The following topics are discussed:

- "Backup and recovery process" on page 242
- "Offline backup and restore using scripts" on page 244
- "Online backup using BRMS" on page 245
- "Scenario 1: Restoring in one step from data saved with a backup policy" on page 291
- "Scenario 2: Restoring individually from data saved with a backup policy" on page 306
- "Using the BRMS commands for backup and restore" on page 327

© Copyright IBM Corp. 2007. All rights reserved.

6.1 Backup and recovery process

The backup and recovery of a WebSphere Portal Express V6 server is complex if you do not understand what to back up. Planning for backup and recovery of your WebSphere Portal Express V6 server involves planning for all of the components that make up the WebSphere Portal Express V6 environment.

The System i platform allows for multiple WebSphere Portal Express profiles on a single system. This means the product data and code common to all profiles are stored in a different location from the data specific to an individual profile. Similarly, each profile's data and configuration are stored in separate locations. Generally, the LDAP server, the HTTP server, and the WebSphere Portal Express V6 server make up the WebSphere Portal Express V6 environment.

This chapter presents information relevant to the backup and restore process of an individual WebSphere Portal Express V6 profile's configuration and user data that reside primarily on the same i5/OS server.

WebSphere Portal Express V6 product data, code, and program files common to all profiles on i5/OS are stored in the i5/OS integrated file system directory of /QIBM/ProdData/PortalExpress/V6. This data rarely changes and most changes usually occur after an upgrade. You can save this directory with a general system save. A schedule of a monthly or quarterly save or after any upgrades is sufficient.

The data for the LDAP server is stored in different places depending on the LDAP server that you are using. See the product documentation for the LDAP server that you are using for information about backup and recovery and the frequency of any backup:

- If you are using the IBM Directory Server for i5/OS as your LDAP server, you can obtain information about saving and restoring directory server information in the System i Information Center at:

  `http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzahy/rzahybup-rf.htm`

- For information about saving and restoring a Domino server on System i, see Chapter 9 of *Implementing IBM Lotus Domino 7 for i5/OS*, SG24-7311, at:

  `http://www.redbooks.ibm.com/abstracts/sg247311.html`

- For information about Microsoft Active Directory backup and restore, see the following Web site at:

  `http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/distrib/dsbj_brr_ixwo.mspx?mfr=true`

While you can run a WebSphere Portal Express server without an external HTTP server, the default external HTTP server used by the WebSphere Portal Express V6 server is the IBM HTTP Server for i5/OS (powered by Apache). This is stored in the /www/*<webserver>* directory.

The WebSphere Portal Express V6 user data is stored in schemas within DB2 for i5/OS. There are default names for the schemas and their parent libraries. These are based on the purpose of the libraries. However, the names of the libraries that contain the schemas depend on the naming option chosen in the Create WebSphere Portal wizard and is based on the server name of the WebSphere Portal Express V6 server. We recommend that you save these libraries daily.

Table 6-1 summarizes the information to be saved and the recommended frequency of the backup.

Table 6-1 Summary of backup recommendations for WebSphere Portal Express V6

Component to be saved	Where data is stored	Frequency of backup
WebSphere Portal Express V6 product data	/QIBM/ProdData/Portal Express/V6	Monthly or quarterly or after upgrades
IBM HTTP Server for i5/OS	/www/<*webserver*>	Daily or weekly
WebSphere Portal Express V6 configuration data	/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*> /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/profileregistry/	Daily
WebSphere Portal Express V6 user data	DB2 Universal Database libraries and schemas	Daily
Database owner user profile and security data	A saved file output of SAVSECDTA	Daily

The product data is used by all WebSphere Portal profiles on i5/OS. In this chapter, we are primarily concerned with individual profiles. In general, the data that has to be saved for a backup for an individual profile includes:

- The i5/OS integrated file system directories and files of the WebSphere Portal Express V6 profile:
  - /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>
  - /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/profileregistry

    Primary files are profileregistry.xml and fsdb/<*profilename*>.
- All WebSphere Portal Express database schemas associated with the profile with the default local schema names:
  - Release database: *LOCAL/REL60
  - Customization database: *LOCAL/CUST60
  - Community database: *LOCAL/COMM60
  - JCR database: *LOCAL/JCR60
  - WMM database: *LOCAL/*DBUser* (replace *DBUser* with the value in the wpconfig_dbdomain.properties file)
  - Feedback database: *LOCAL/FDB60
  - Likeminds database: *LOCAL/LKM60
- The external HTTP server associated with the profile, if there is one:
  - A single record member in file QUSRSYS/QATMHINSTC, named <*webserver*>, pointing to the location of the HTTP configuration data
  - i5/OS integrated file system objects in /www/<*webserver*> for the HTTP server
- User profile information. There is no simple way to save a single user profile, so all user profiles are saved using the Save Security Data (SAVSECDTA) CL command even though we are only interested in one user profile.

Note: You only restore the single user profile associated with the WebSphere Portal Express profile.

There are three methods of backing up your WebSphere Portal Express V6 environment:

- A general system backup that saves everything on your system.
- Offline backup using WebSphere Portal Express V6 scripts. See 6.2, “Offline backup and restore using scripts” on page 244 for more information.
- Online backup using Backup, Recovery and Media Services (BRMS). See 6.3, “Online backup using BRMS” on page 245 for more information.

Each of the three routines mentioned has its own benefits. We will not discuss the various routines except to mention that offline backup of the WebSphere Portal Express V6 server is the best and most effective way to ensure that all data related to your profile is backed up.

6.2 Offline backup and restore using scripts

This chapter documents a process to back up a portal server while it is online and in use. However, it is worth mentioning the need to do offline backup with scripts. Offline backup remains the best way to ensure that all your data is completely saved. There is extensive documentation on how to perform offline backups using scripts. See *Backup and restore on i5/OS* information in the WebSphere Portal Express V6 Information Center at:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp?topic=/com.ibm.wp.exp.doc/wpf/i_wadm_c_backup_inst_i5os.html

The backup and restore scripts are found in the /QIBM/ProdData/PortalExpress/V6/Tools/ directory. The folder contains many save and restore related scripts, but the primary scripts are:

- savWpProfile.sh - saves the base WebSphere Portal Express servers
- rstWpProfile.sh- restores the base WebSphere Portal Express servers

6.2.1 Example of an offline backup

A general offline backup requires that the WebSphere Portal server is stopped.

For base servers, use the savWpProfile.sh script (for ND servers, use the savNdProfile.sh script).

From the QShell environment (STRQSH command), enter the following commands:

```
cd /QIBM/ProdData/PortalExpress/v6/Tools
savWpProfile.sh –profileName wp6xserver –saveFileLib wp1lib –logDir /mywp1logs
```

Where:

- *wp6xserver* is the WebSphere Portal Express V6 profile being saved.
- *wp1lib* is the save file library where the save files are created. If it does not exist, it will be created. Most, if not all, data in this library will be overwritten, so do not reuse the same library name.

- *mywp1logs* is the i5/OS integrated file system directory where the logs will go (it is created if not there). It is *critical* to keep the save logs so you can examine them if a problem occurs with a future restore.

Note: To perform this task, you need an i5/OS user profile with special authorities of *ALLOBJ, *SAVSYS, and *IOSYSCFG.

See *Backing up a profile on i5/OS* in the WebSphere Portal Express V6 Information Center for more complex examples and a detailed discussion of the savWpProfile.sh script:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp?topic=/com.ibm.wp.exp.doc/wpf/i_wadm_c_backup_inst_i5os.html

6.2.2 Example of restore using scripts

This section shows an example of restoring a WebSphere Portal profile using scripts. For base servers, use the rstWpProfile.sh script. For ND servers, use the rstNdProfile.sh script.

From the QShell environment (STRQSH command), enter the following commands:

```
cd /QIBM/ProdData/PortalExpress/v6/Tools
rstWpProfile.sh –p wp6xserver –s wp1lib –l /mywp1logs
```

Where:

- *wp6xserver* is the WebSphere Portal Express V6 profile being restored.
- *wp1lib* is the save file library where the save files are located.
- *mywp1logs* is the i5/OS integrated file system directory where the logs will go (it is created if not there). It is *critical* to keep the save logs so you can go back and see what happened at save time if a problem occurs.

Restore is a more complex function than save. Existing profile data needs to be cleared off the system prior to the restore and care must be taken to recover the existing profile if there was a mistake. This is called *safety net* processing. For a detailed discussion about safety net processing and the restore process in general, see *Restoring a profile on i5/OS* in the WebSphere Portal Express V6.0 Information Center at:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp?topic=/com.ibm.wp.exp.doc/wpf/i_wadm_t_restore_inst_i5os.html

6.3 Online backup using BRMS

This section introduces a way to back up the WebSphere Portal server while it is online. Then in later sections of this chapter, we restore the data that was backed up. This is done using the Backup, Recovery, and Media Services (BRMS) product. BRMS on i5/OS is a separately purchased product that assists you in defining and processing your backup, recovery, and media management operations. For more information about BRMS, see the Backup Recovery and Media Services for iSeries document at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc415345.pdf

The following prerequisite hardware and software list is required to install and use the BRMS client. For more information, see the *Backup Recovery and Media Services for iSeries, BRMS iSeries Navigator Client Student Guide* at:

http://www.ibm.com/servers/eserver/iseries/service/brms/pdf/StudentGuide54.pdf

Workstation (PC):

- Processor: 850 MHz or faster
- Memory: 512 MB is recommended
- Disk space: 1 GB or more of unused DASD
- Display: Minimum resolution of 800 x 600 (1024 x 768 is recommended)
- Operating system: Windows 2000/XP
- Software: IBM iSeries Access for Windows

i5/OS:

- Operating System/400® (5722-SS1)
- Operating System/400 Option 18, Media Storage Extensions
- IBM iSeries Access for Windows (5722-XE1)
- Backup Recovery and Media Services (5722-BR1)
- Latest PTFs applied for all installed software

The BRMS client is installed as a plug-in within the iSeries Navigator. Consult the *BRMS iSeries Navigator Client Student Guide* for installing the plug-in if you do not have it installed.

We use the BRMS iSeries Navigator client in our example. The *BRMS iSeries Navigator Client Student Guide* explains in detail all the capabilities of the BRMS iSeries Navigator Client. We recommend you use this resource as a guide as we go through the examples. We do not discuss much of either the BRMS product or the client. Most of the directions are taken from the *BRMS iSeries Navigator Client Student Guide*.

Tip: Everything we do with the BRMS client in this section can also be done with a 5250 emulation session. As we go through the example, we point out, in some instances, a corresponding command in the 5250 emulation session.

A *backup policy* is a set of defaults that controls what information is backed up by BRMS, how it is backed up, and where it is backed up. You can also specify options to control what happens before, during, and after the backup. You can control the following backup policy options:

- What backup items you want to include in the policy and what type of backup you want to perform on those items.
- Whether you want to shut down your integrated servers before the backup begins, and whether you want to restart them after the backup completes.
- Whether you want to unmount user-defined file systems before the backup begins.

For our example, we go through a sample process to create a backup policy to back up a WebSphere Portal Express V6 profile while it is active. We will use the BRMS client to perform the following steps:

1. Create a backup policy with the following properties:
   - It is an online backup, meaning the profile is in active use. Save While Active features are implemented. Objects are saved in ragged state, meaning we do not wait for pending transactions to commit or rollback. Instead, we save as is. The necessary rollback or roll forward activities for uncommitted transactions are dealt with by the restore process. This makes for a quicker save.
   - The backup is customized to use both full and cumulative changes. A full save is done for all libraries everyday. A full save is done for integrated file system objects on one day per week (Sunday, usually), and the cumulative changes (changes since last full

save) are done for every other day of the week it is run. We choose to perform full daily saves for all libraries and library objects because saving libraries is a fairly quick process. It is also where most of the user data resides. We perform cumulative saves for the various stream files because those files are fairly static and do not change much. We choose a full and cumulative save as opposed to full and incremental save for ease of restore.

   – We save to a tape or virtual tape and show examples within the process where there is a difference between the two. Note also that you can use various other media. We use tape in our example because it makes for an easier demonstration process.

2. Schedule the backup job to run daily. Because it is a customized backup, it performs full backup or only a cumulative changes backup, depending on the day of the week.
3. Run an online backup of WebSphere Portal Express V6.

Before you run through the examples in this section, you *must* download the following scripts. See details about downloading these scripts in Appendix B, “Additional material” on page 359. You must transfer the files to the i5/OS integrated file system directory, /QIBM/ProdData/PortalExpress/V6/Tools:

- ExpressSave.sh: This script collects the private authorities of all objects (for QTMHHTTP and QEJBSRV) before they are saved. It also runs the Save Security Data (SAVSECDTA) CL command to collect the profile’s database administrator’s user profile to a save file. The output files are saved with the backup and subsequently deleted.
- PreExpressRestore.sh: This script is only used as a cleanup script prior to a restore where you want to restore all libraries and integrated file system objects.
- PostExpressRestore.sh**:** This script restores the private authorities of all integrated file system objects (for QTMHHTTP and QEJBSRV) that were collected when the backup was run. It also restores the user profile that owns the databases associated with the profile being restored. The private authority of the user profile is also restored.

6.3.1 Creating a backup policy using the Backup Policy wizard

Before you create a backup policy, you need to know the exact data to be saved. See the following list for the sample data to save. Also see 6.1, “Backup and recovery process” on page 242.

For a profile called WP6XSERVER**,** following are the folders, their subfolders, and objects to be saved:

- Profile data:

```
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER
/QIBM/UserData/WebSphere/AppServer/V6/Base/profileRegistry/FSDB/WP6XSERVER
/QIBM/UserData/WebSphere/AppServer/V6/Base/profileRegistry/profileregistry.xml
```

- Schemas: WP6XADMIN, WPECMM3, WPECST3, WPEFDB3, WPEJCR3, WPELKM3, and WPEREL3

  Note: You can get a list of the schemas or libraries associated with the WebSphere Portal profile by using the following QShell command:

  ```
  /QIBM/ProdData/PortalExpress/V6/Tools/sh_utils/getListWpsSchemas.sh
  <profilename>
  ```

  For example:

  ```
  /QIBM/ProdData/PortalExpress/V6/Tools/sh_utils/getListWpsSchemas.sh
  WP6XSERVER

  WP6XADMIN WPECMM3 WPECST3 WPEFDB3 WPEJCR3 WPELKM3 WPEREL3
  ```

  Tip: When you use the getlistWpsSchemas.sh script, the first entry in the result list in our example, `wp6xadmin`, has the same name as the user profile that owns the databases associated with the WebSphere Portal profile.

- Objects:
  - WP6XWEB member in file QUSRSYS/QATMHINSTC
  - QGPL/USERPROFS save file

  Note: Use the QGPL/USERPROFS save file to save all user profiles and security data. You *must* manually create this save file using the following i5/OS command:

  ```
  CRTSAVF FILE(QGPL/USERPROFS)
  ```

The following command determines the HTTP server that is used with the WebSphere Portal profile, if any:

```
/usr/bin/java -cp

/qibm/proddata/httpa/java/lib/wasadmin.jar:/QIBM/ProdData/PortalExpress/V6/Tools/l
ib/i5tools.jar:/qibm/proddata/os400/jt400/lib/jt400native.jar:/QIBM/ProdData/Porta
lExpress/V6/Tools/lib/AdminExp.jar:/QIBM/ProdData/PortalExpress/V6/Tools/lib/Admin
Toolkit.jar:/QIBM/ProdData/PortalExpress/V6/Tools/lib/AdminGui.jar findHTTP
WP6XSERVER /QIBM/UseRData/WebSphere/Appserver/V6/Base/profiles/WP6XSERVER/HTTP.rc
```

In this example, WP6XSERVER is the HTTP server. The output file to inspect for your HTTP server is:

```
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/HTTP.rc
```

Note: For 5250 emulation session users, use the Work with Backup Control Groups (WRKCTLGBRM) command to create a policy, specify the items to be saved, the tape device to be used, the media policy to be used, and so on. These are the same activities we perform with the BRMS client in this example.

To create the Backup Policy, perform the following steps:

1. From the iSeries Navigator, expand **Backup, Recovery and Media Services**, right-click **Backup Policy** and select **New Policy** (Figure 6-1).

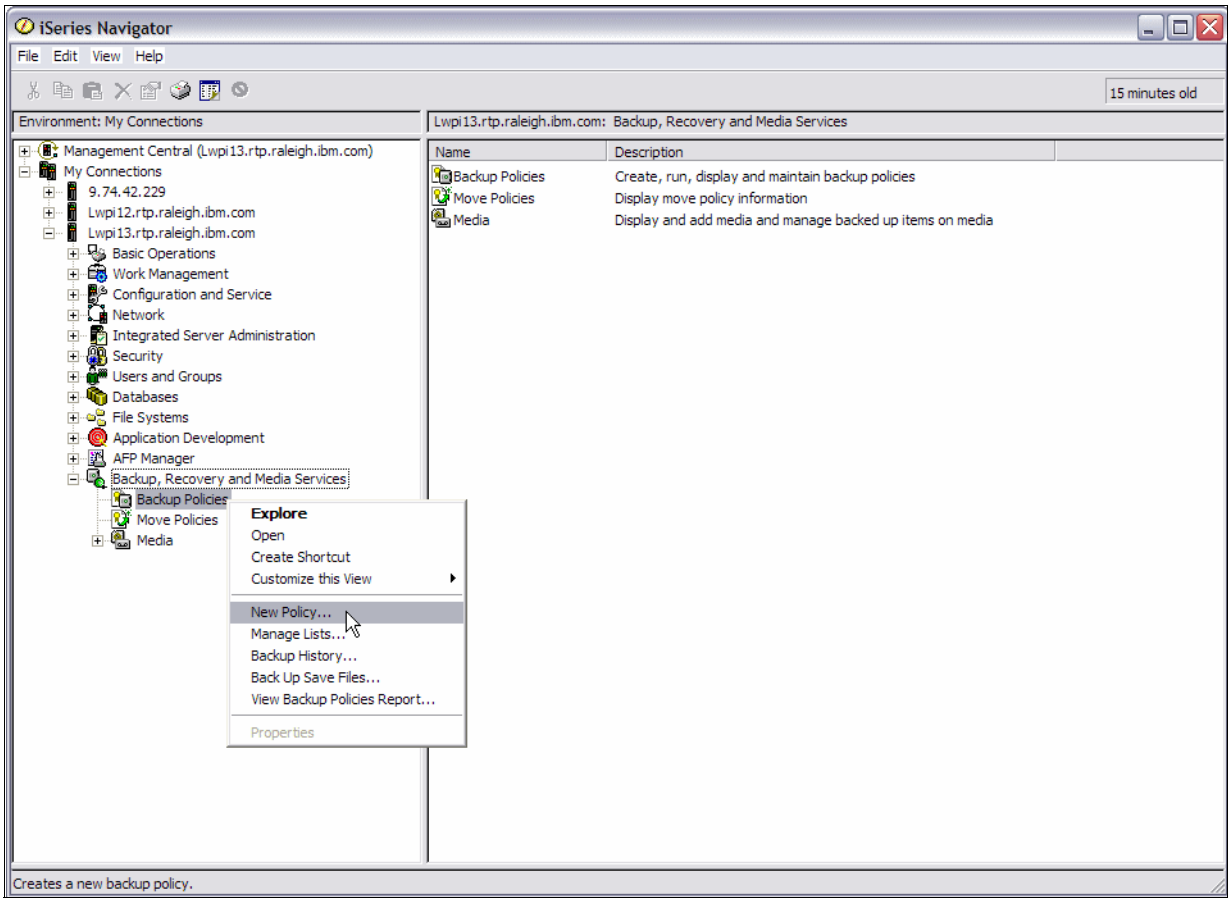


Figure 6-1 Creating a new policy

2. A welcome window is displayed (Figure 6-2). Click **Next**.

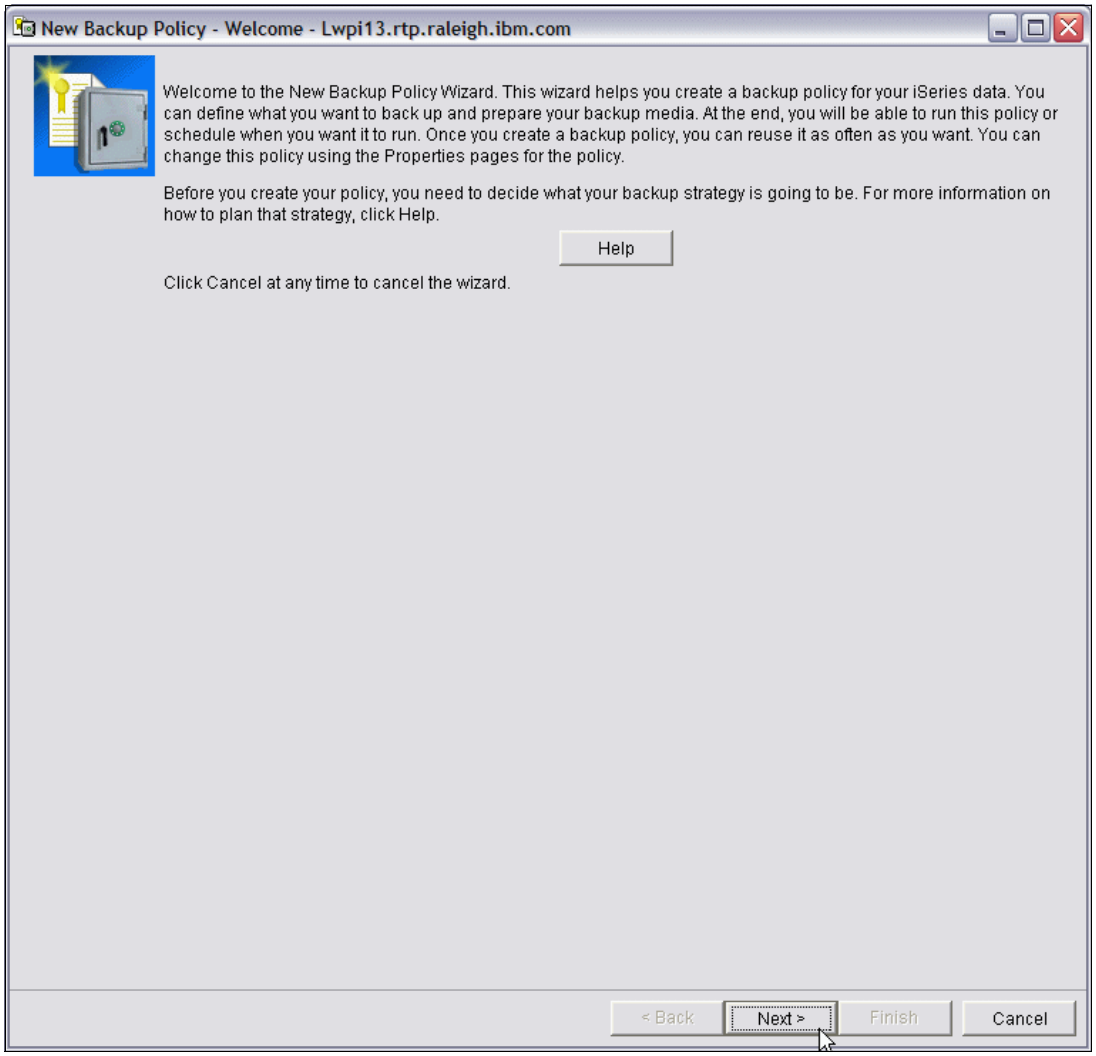

New Backup Policy - Welcome - Lwpi13.rtp.raleigh.ibm.com
Welcome to the New Backup Policy Wizard. This wizard helps you create a backup policy for your iSeries data. You can define what you want to back up and prepare your backup media. At the end, you will be able to run this policy or schedule when you want it to run. Once you create a backup policy, you can reuse it as often as you want. You can change this policy using the Properties pages for the policy.
Before you create your policy, you need to decide what your backup strategy is going to be. For more information on how to plan that strategy, click Help.
Help
Click Cancel at any time to cancel the wizard.
< Back
Next >
Finish
Cancel

Figure 6-2 Welcome window

3. Enter the name and description of the backup policy and click **Next** (Figure 6-3). In our example, the backup policy name is `WP6XPOLICY`.

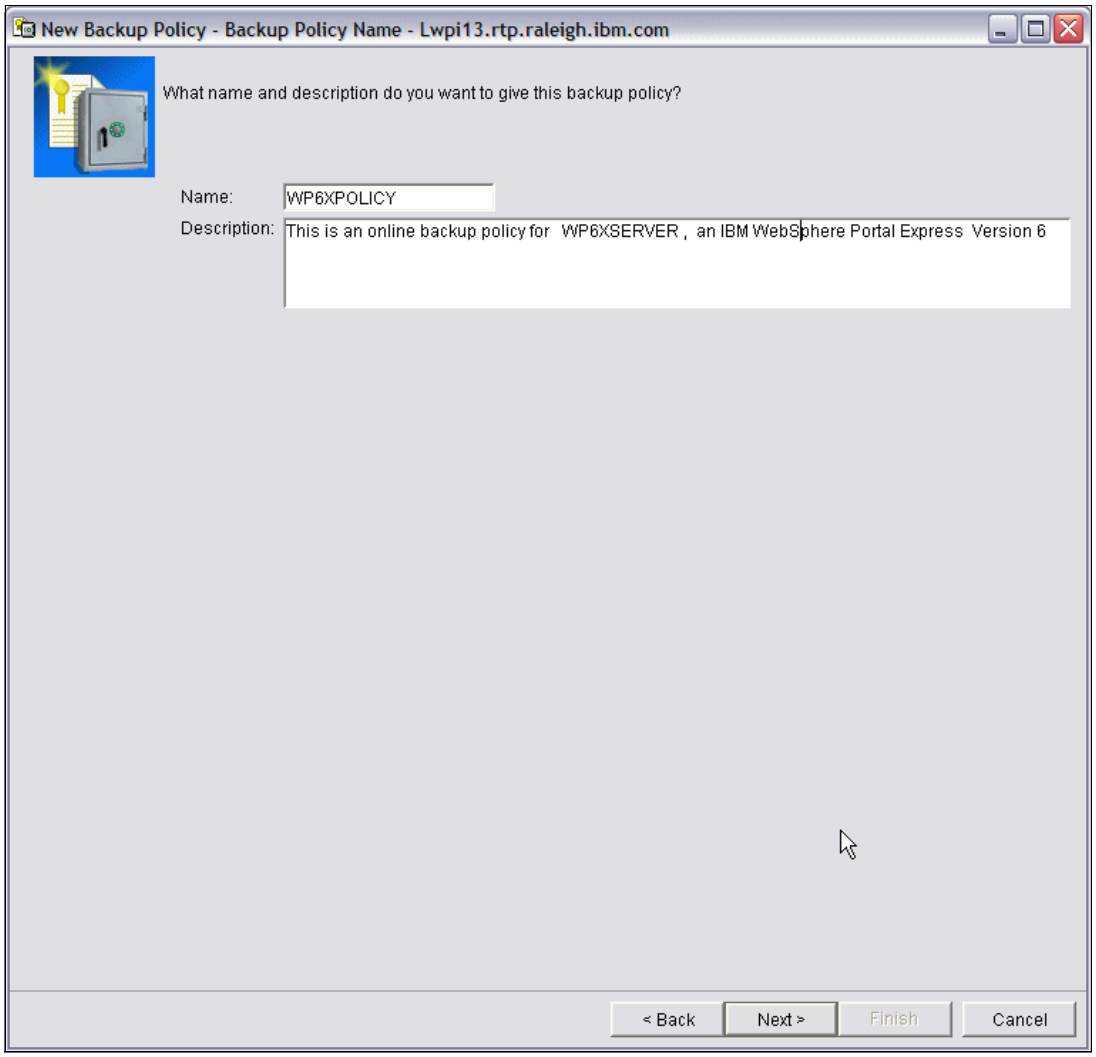

New Backup Policy - Backup Policy Name - Lwpi13.rtp.raleigh.ibm.com
What name and description do you want to give this backup policy?
Name:
WP6XPOLICY
Description:
This is an online backup policy for WP6XSERVER , an IBM WebSphere Portal Express Version 6
< Back
Next >
Finish
Cancel

Figure 6-3 Entering a name for the backup policy

4. On the Select a Backup Strategy window, save the custom data by selecting **Back up Lotus server data or a customized set of objects** (Figure 6-4). Click **Next**.

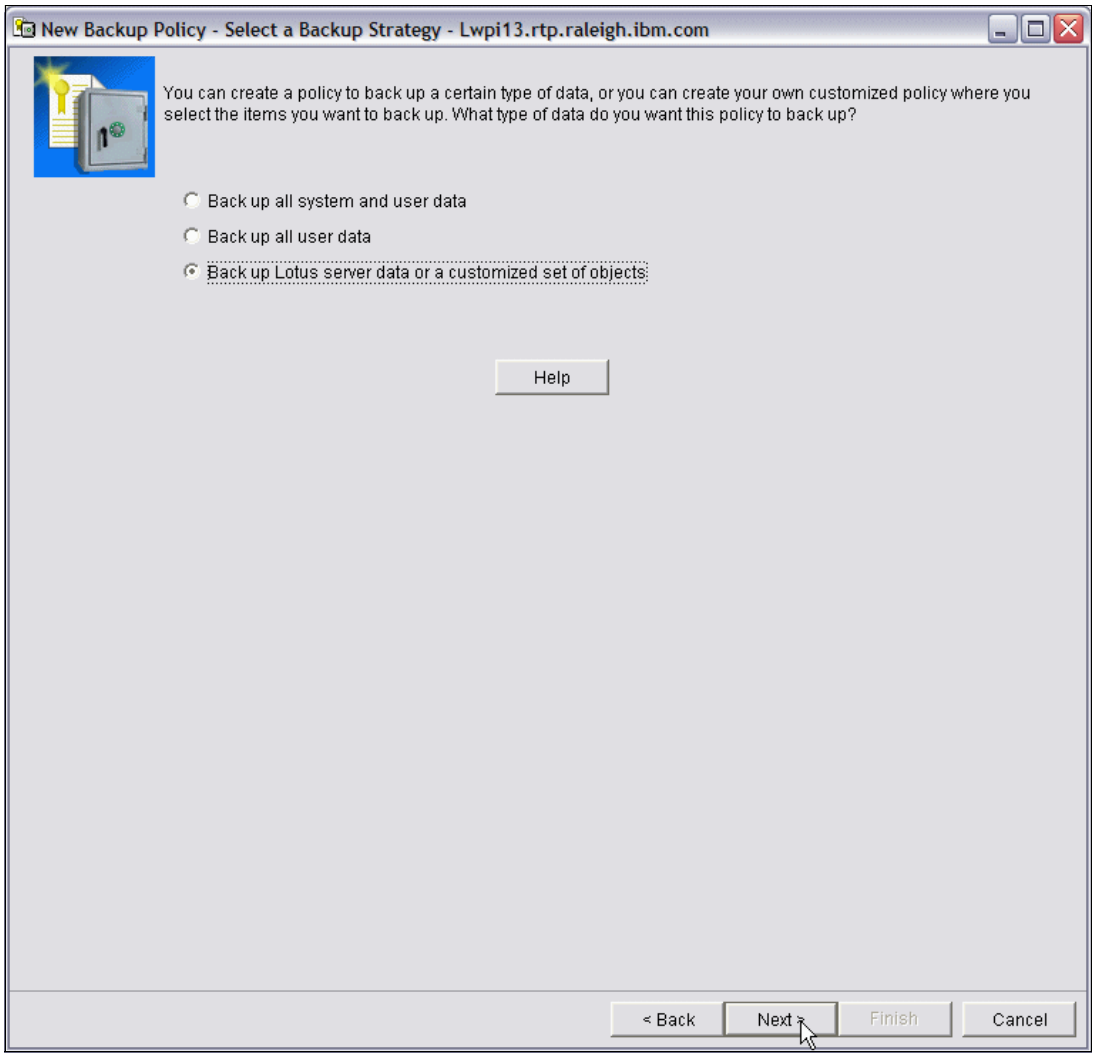

New Backup Policy - Select a Backup Strategy - Lwpi13.rtp.raleigh.ibm.com
You can create a policy to back up a certain type of data, or you can create your own customized policy where you select the items you want to back up. What type of data do you want this policy to back up?
Back up all system and user data
Back up all user data
Back up Lotus server data or a customized set of objects
Help
< Back
Next >
Finish
Cancel

Figure 6-4 Selecting a backup strategy

5. On the Customize IBM Data or User Data window, select **User data** and click **Next** (Figure 6-5).

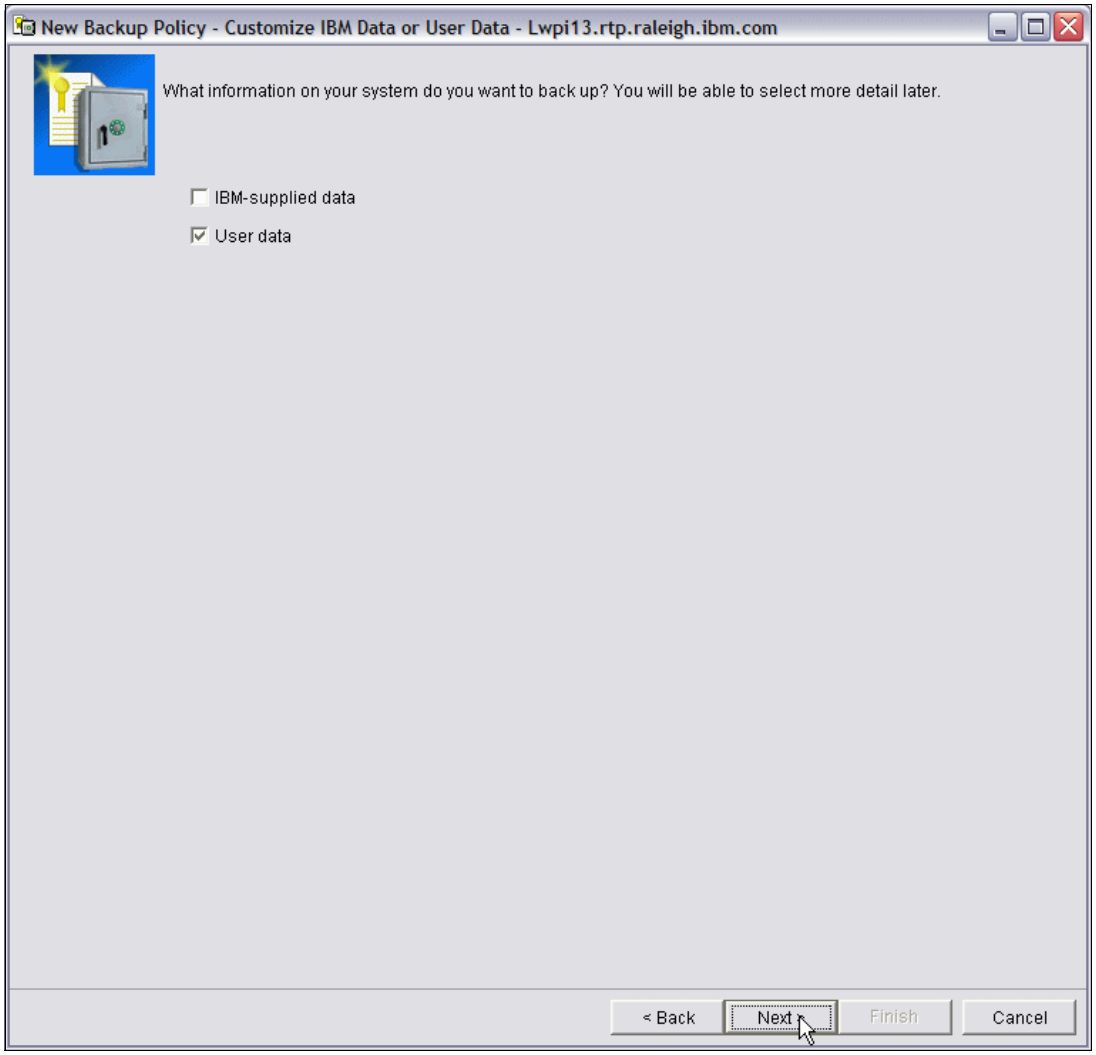

New Backup Policy - Customize IBM Data or User Data - Lwpi13.rtp.raleigh.ibm.com
What information on your system do you want to back up? You will be able to select more detail later.
IBM-supplied data
User data
< Back
Next >
Finish
Cancel

Figure 6-5 Selecting user data to customize

6. On the Customize User Data window, click **Select specific items for backup** and click **Next** (Figure 6-6).

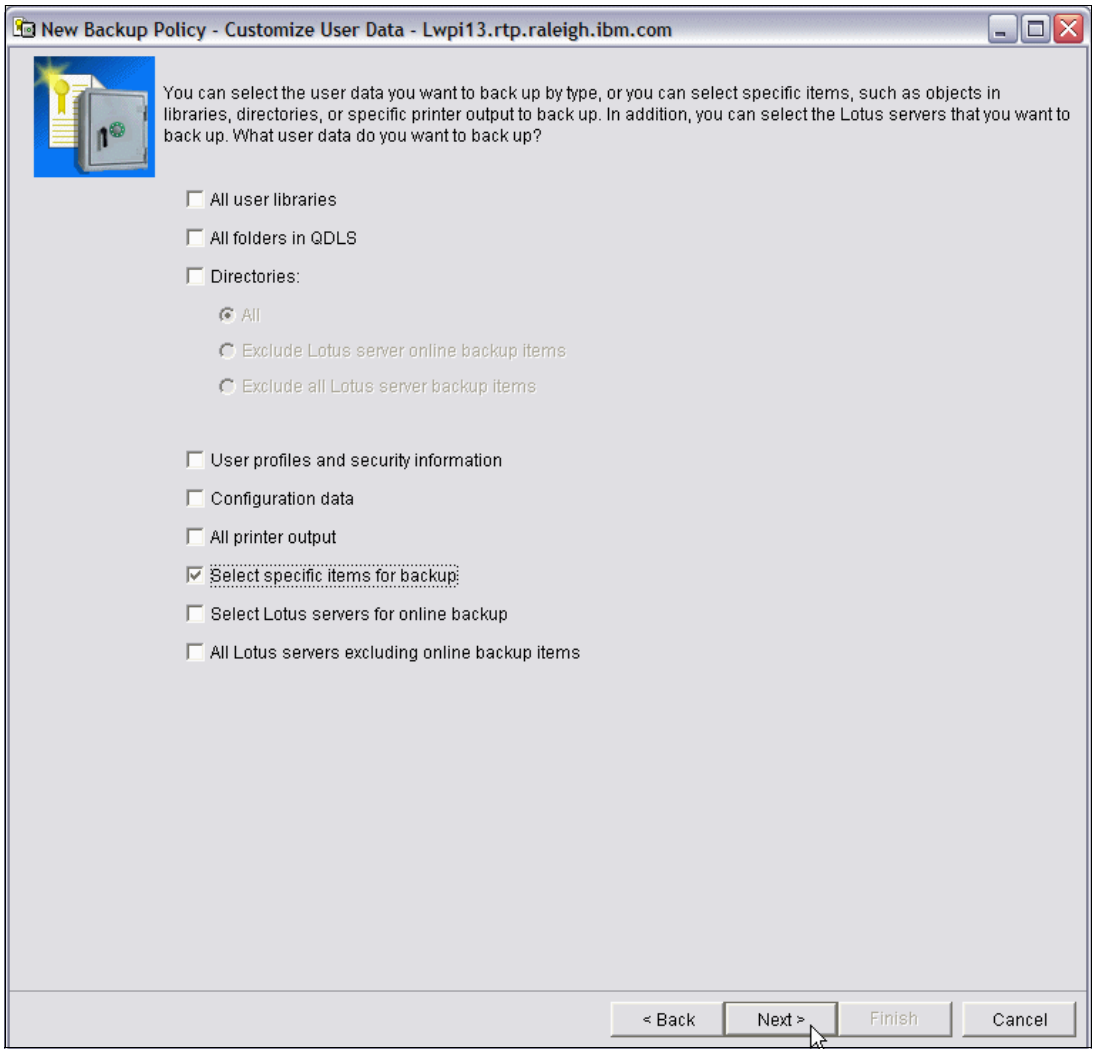

New Backup Policy - Customize User Data - Lwpi13.rtp.raleigh.ibm.com
You can select the user data you want to back up by type, or you can select specific items, such as objects in libraries, directories, or specific printer output to back up. In addition, you can select the Lotus servers that you want to back up. What user data do you want to back up?
All user libraries
All folders in QDLS
Directories:
All
Exclude Lotus server online backup items
Exclude all Lotus server backup items
User profiles and security information
Configuration data
All printer output
Select specific items for backup
Select Lotus servers for online backup
All Lotus servers excluding online backup items
< Back
Next >
Finish
Cancel

Figure 6-6 Specifying that specific items will be saved

7. On the Select Items for Backup window, you select all the data you intend to save:

   a. For the directory containing the external HTTP server data, in our example, expand **www** and select **wp6xweb**. See Figure 6-7.

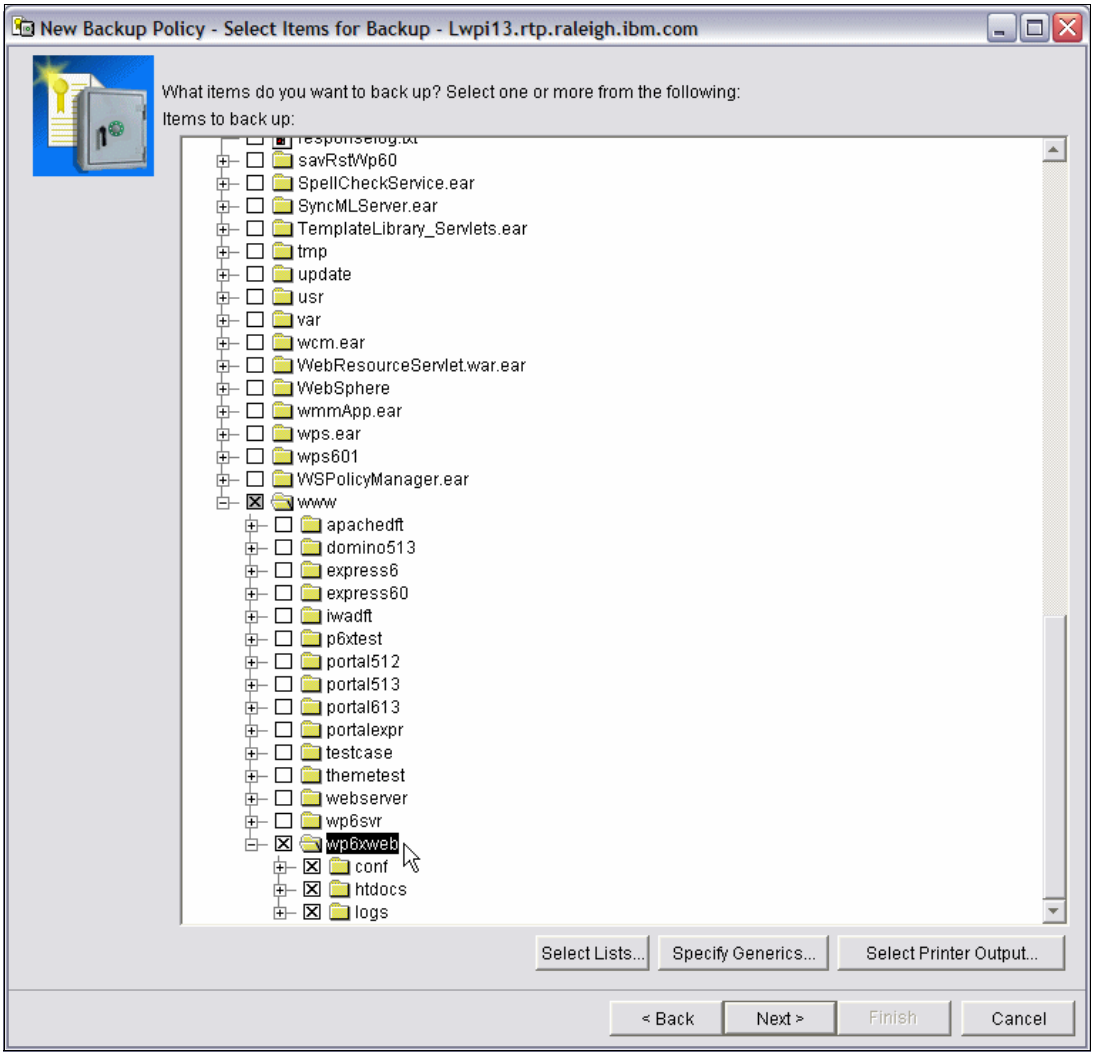


Figure 6-7 Selecting the HTTP server

b. For the directory containing the WebSphere Portal Express V6 profile data, /QIBM/UserData/Websphere/Appserver/v6/Base/profiles/WP6XSERVER, expand **QIBM** → **UserData** → **WebSphere** → **AppServer** → **V6** → **Base** → **profiles** and select **WP6XSERVER** (Figure 6-8).

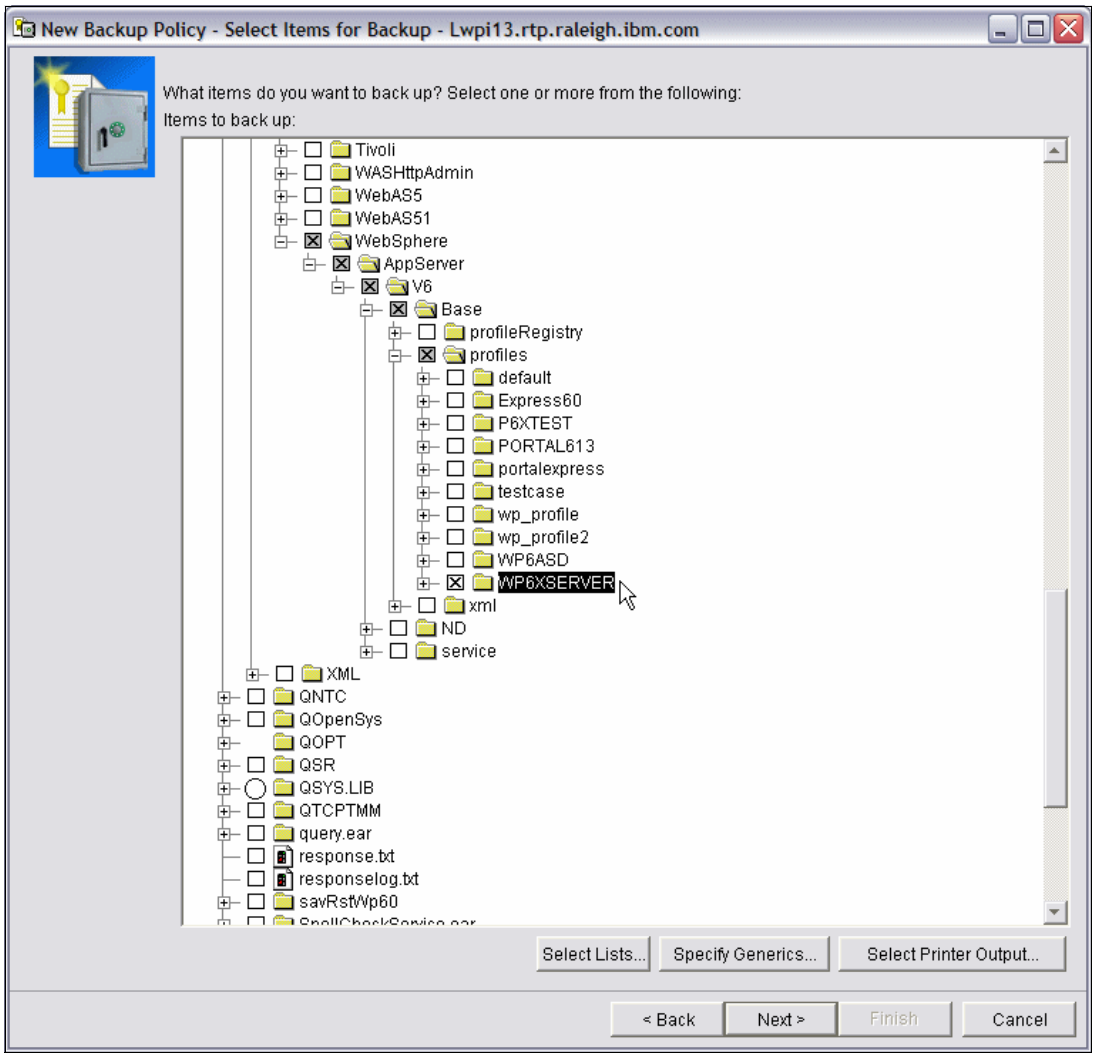


Figure 6-8 Selecting the WebSphere Portal Express V6 main profile directory

c. Next, select the profile related information in the profile registry folder of /QIBM/UserData/Websphere/Appserver/V6/Base/ProfileRegistry/fsdb/WP6XSERVER by expanding **QIBM** → **UserData** → **WebSphere** → **AppServer** → **V6** → **Base** → **profileRegistry** → **fsdb** and selecting **WP6XSERVER** (Figure 6-9).

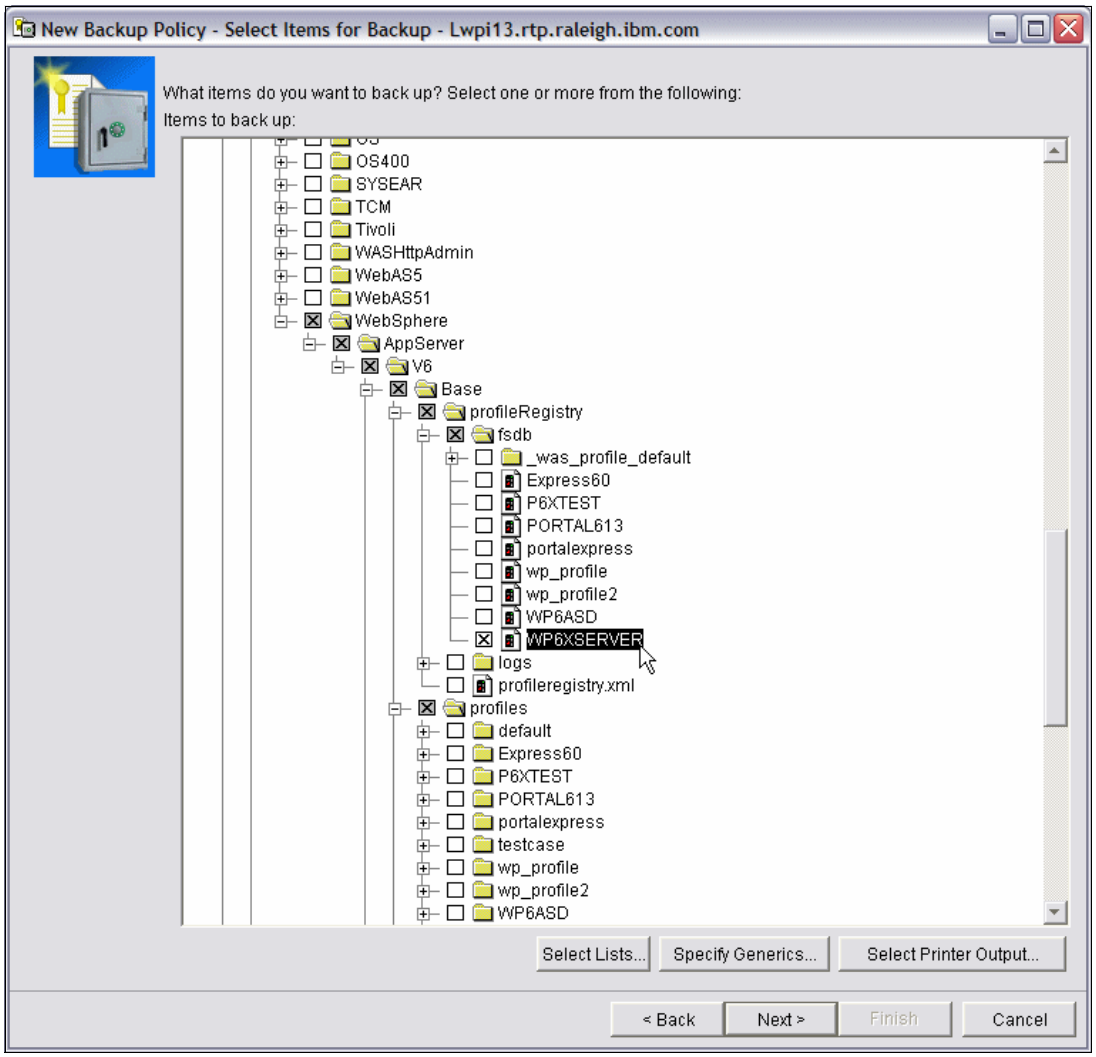


Figure 6-9 Selecting the portal profile's fsdb directory data

d. Select the profileregistry.xml file located in the /qibm/userdata/websphere/appserver/v6/base/profileRegistry/profileRegistry.xml directory by expanding **QIBM** → **UserData** → **WebSphere** → **AppServer** → **V6** → **Base** → **profileRegistry** and selecting **profileregistry.xml** (Figure 6-10).

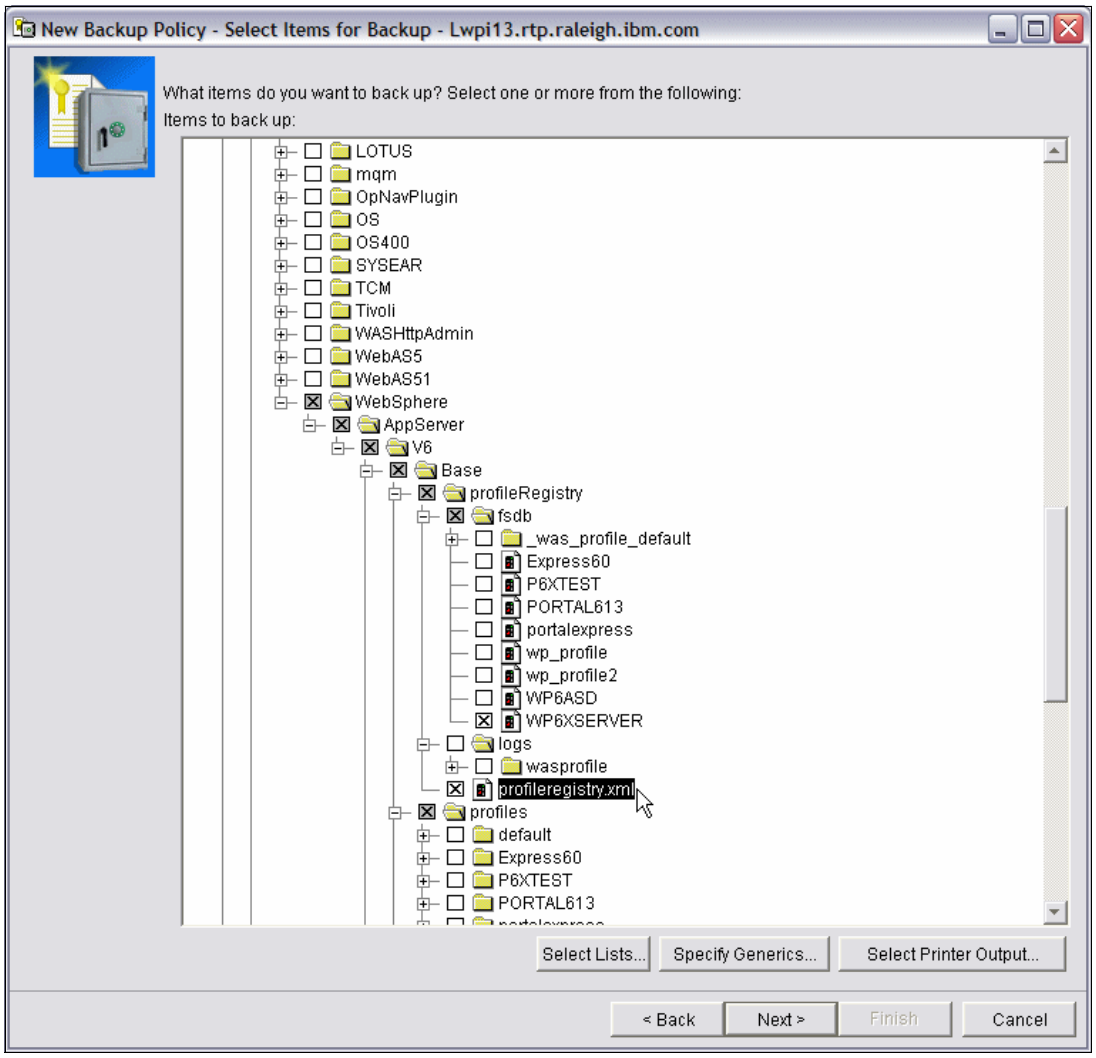


Figure 6-10 Selecting the profileregistry.xml file

e. For the libraries containing the schemas (for our example, this is WP6XADMIN, WPECMM3, WPECST3, WPEFDB3, WPEJCR3, WPELKM3, and WPEREL3), expand **QSYS.LIB** and select all relevant libraries (Figure 6-11).

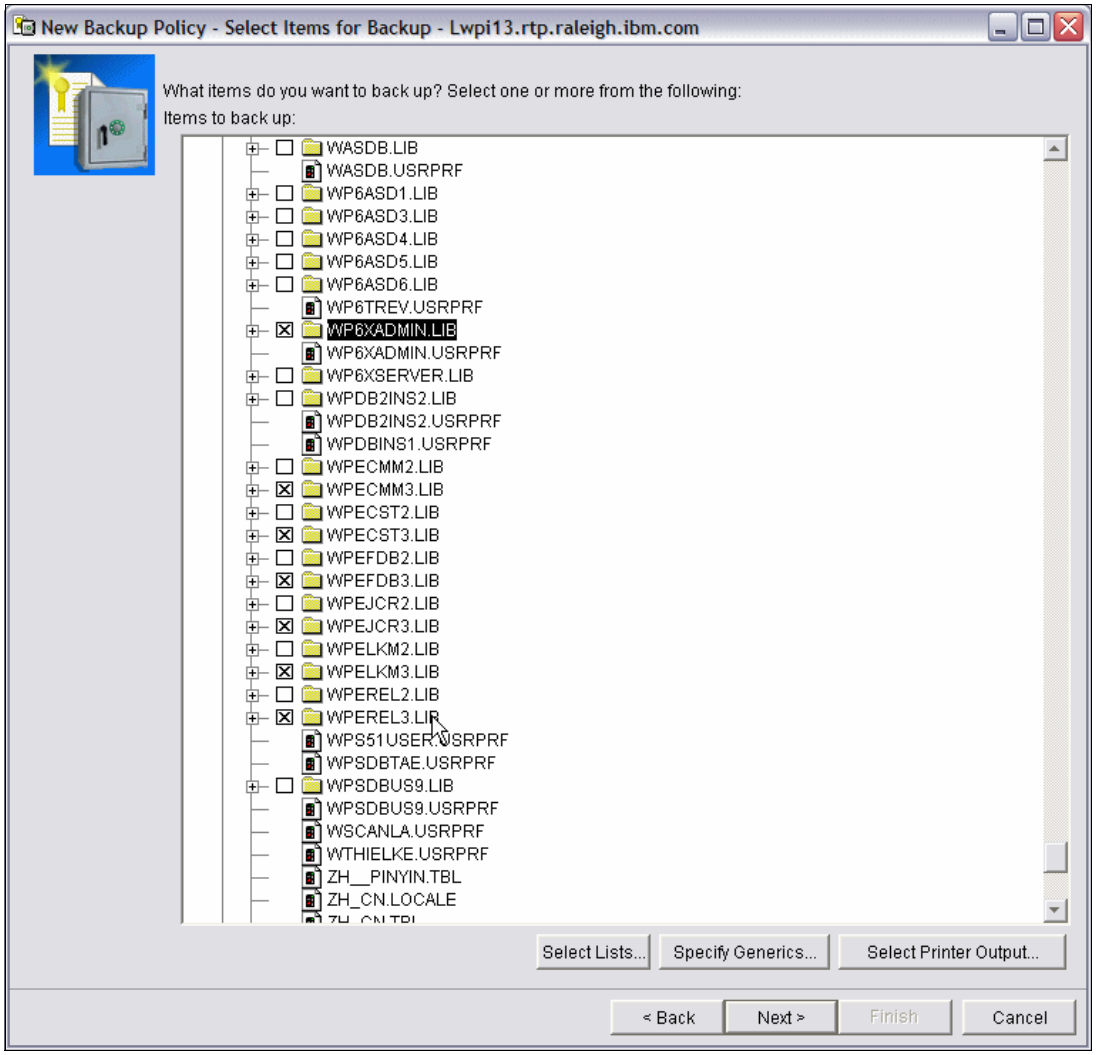


Figure 6-11 Selecting the schema libraries

f. For the WP6XWEB member in QUSRSYS/QATMHINSTC, expand **QSYS.LIB** → **QUSRSYS.LIB** → **QATMHINSTC.FILE** and select **WP6XWEB.MBR** (Figure 6-12).

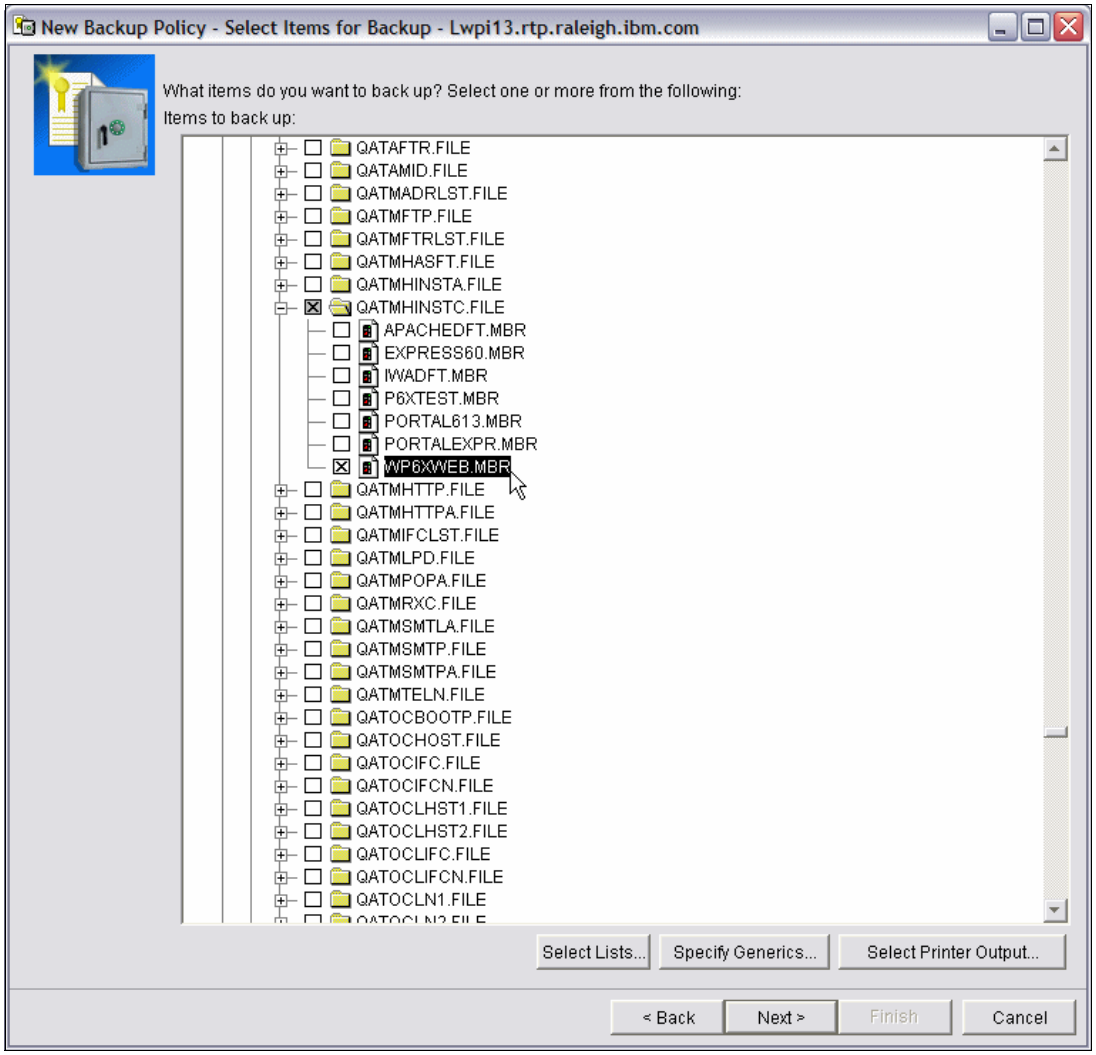


Figure 6-12 Selecting the HTTP member data

g. For the USERPROFS file in QGPL, expand **QSYS.LIB** → **QGPL.LIB** and select **USERPROFS.FILE** (Figure 6-13).

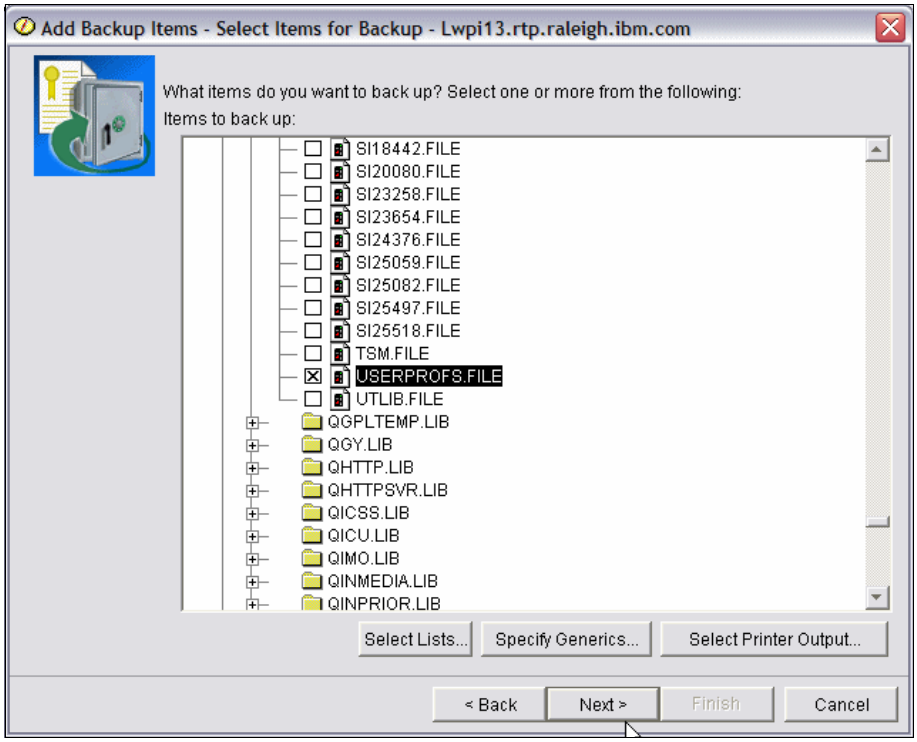


Figure 6-13 Selecting QGPL/USERPROFS save file

h. When you are done selecting all the data, click **Next**.

> **Note:** You are not adding entries you want to omit yet. This follows later when you create an omit list.

8. The next few windows show a summary of what you have selected for your backup. Inspect the HTTP member data and click **Next**. (Figure 6-14).

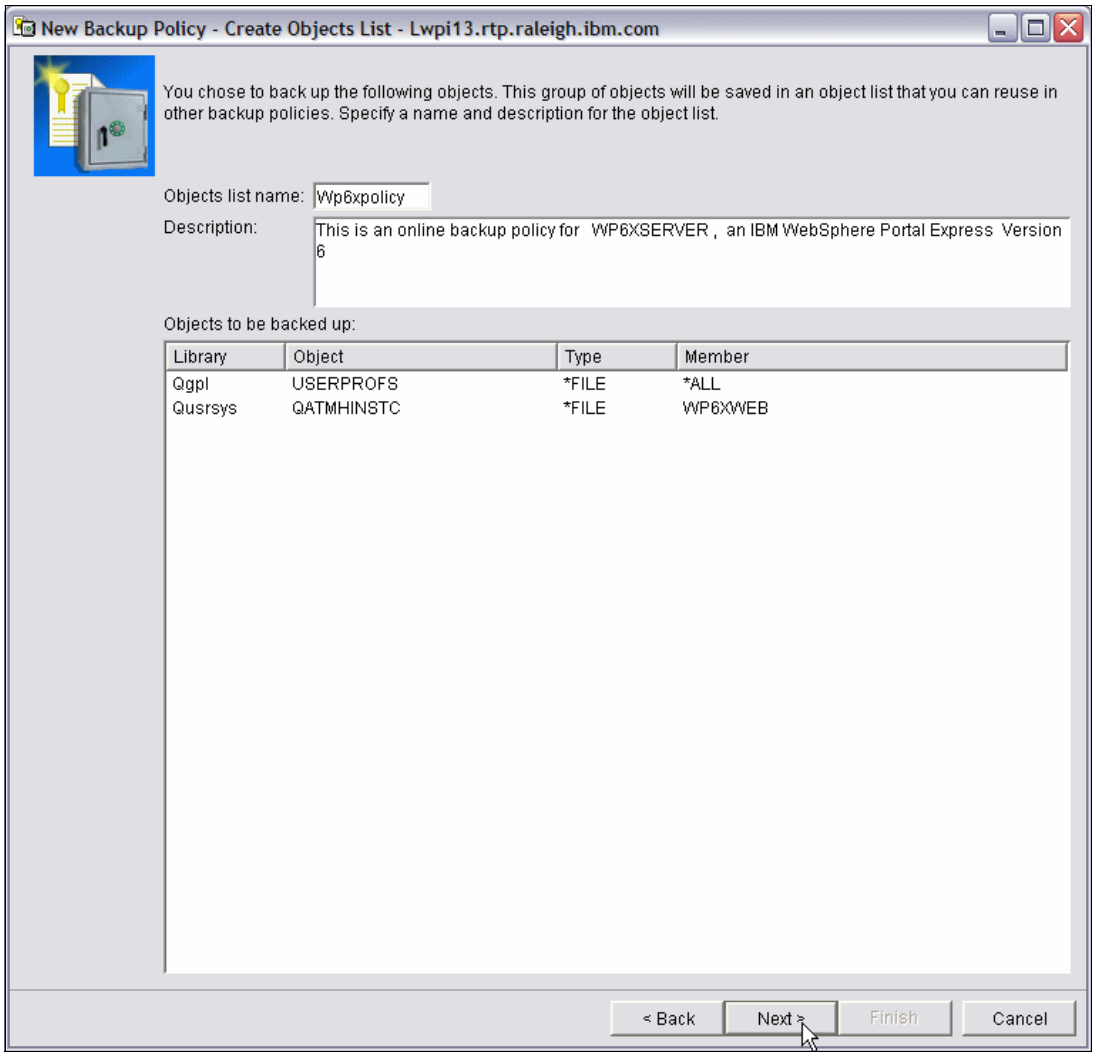

New Backup Policy - Create Objects List - Lwpi13.rtp.raleigh.ibm.com
You chose to back up the following objects. This group of objects will be saved in an object list that you can reuse in other backup policies. Specify a name and description for the object list.
Objects list name:
Wp6xpolicy
Description:
This is an online backup policy for WP6XSERVER , an IBM WebSphere Portal Express Version 6
Objects to be backed up:
Library
Object
Type
Member
Qgpl
USERPROFS
*FILE
*ALL
Qusrsys
QATMHINSTC
*FILE
WP6XWEB
< Back
Next >
Finish
Cancel

Figure 6-14 HTTP member and userprofs data

9. Next, you are shown the directory list selected. Make sure to select the **Include all subdirectories** check box located at the bottom of the window (Figure 6-15). Click **Next.**

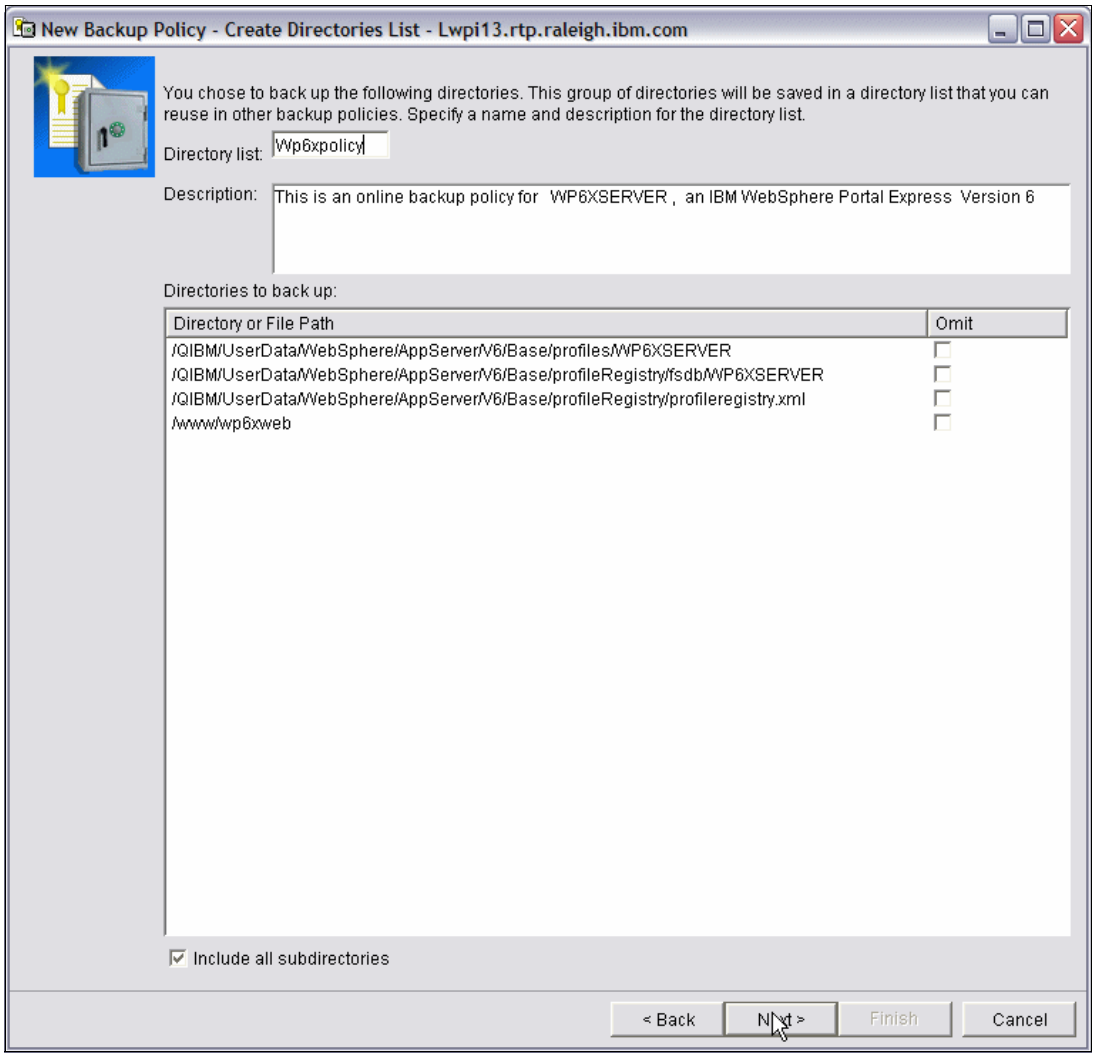

New Backup Policy - Create Directories List - Lwpi13.rtp.raleigh.ibm.com
You chose to back up the following directories. This group of directories will be saved in a directory list that you can reuse in other backup policies. Specify a name and description for the directory list.
Directory list:
Wp6xpolicy
Description:
This is an online backup policy for WP6XSERVER , an IBM WebSphere Portal Express Version 6
Directories to back up:
Directory or File Path
Omit
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER
/QIBM/UserData/WebSphere/AppServer/V6/Base/profileRegistry/fsdb/WP6XSERVER
/QIBM/UserData/WebSphere/AppServer/V6/Base/profileRegistry/profileregistry.xml
/www/wp6xweb
Include all subdirectories
< Back
Next >
Finish
Cancel

Figure 6-15 Verifying the various directories are selected

10. A summary list of selected objects for backup is also displayed (Figure 6-16). Click **Next**.

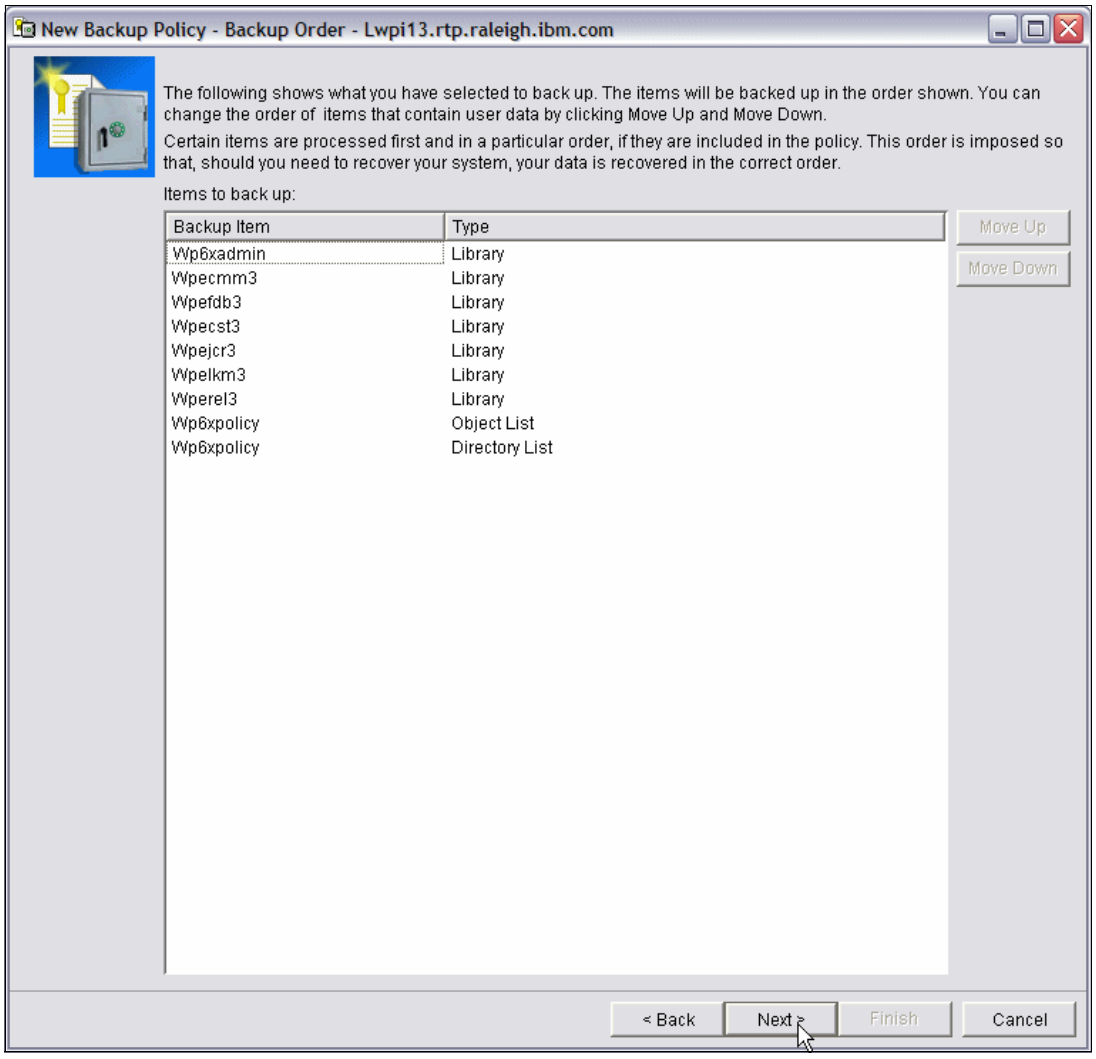

New Backup Policy - Backup Order - Lwpi13.rtp.raleigh.ibm.com
The following shows what you have selected to back up. The items will be backed up in the order shown. You can change the order of items that contain user data by clicking Move Up and Move Down.
Certain items are processed first and in a particular order, if they are included in the policy. This order is imposed so that, should you need to recover your system, your data is recovered in the correct order.
Items to back up:
Backup Item
Type
Wp6xadmin
Library
Wpecmm3
Library
Wpefdb3
Library
Wpecst3
Library
Wpejcr3
Library
Wpelkm3
Library
Wperel3
Library
Wp6xpolicy
Object List
Wp6xpolicy
Directory List
Move Up
Move Down
< Back
Next >
Finish
Cancel

Figure 6-16 Summary list of selected objects

11. Next, you are presented with an option to determine the nature of the backup. You perform a customized backup of both full and changes only. For now, select the defaults of **Full Backup** and **Changes since last full backup (cumulative)**. Click **Next** (Figure 6-17).

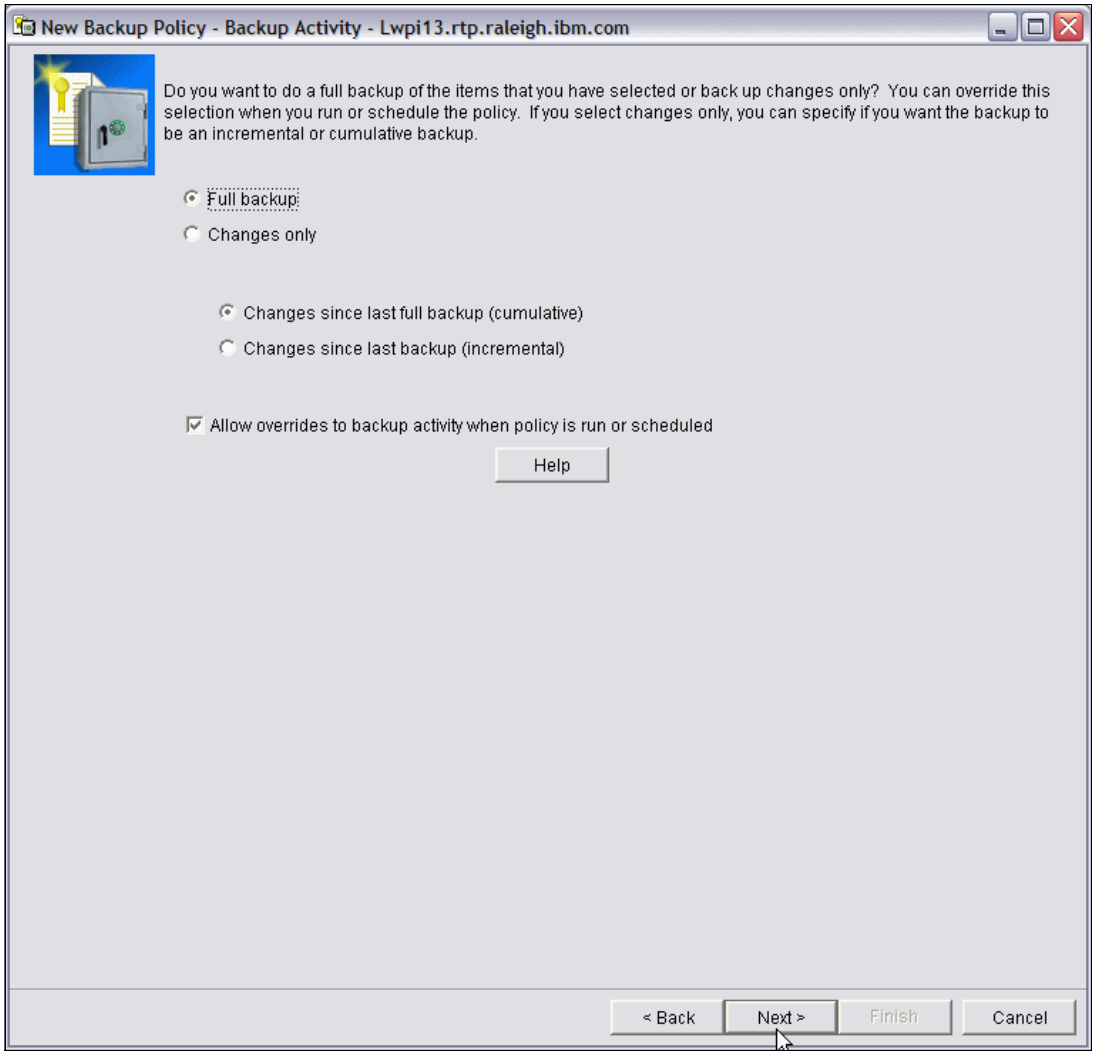

New Backup Policy - Backup Activity - Lwpi13.rtp.raleigh.ibm.com
Do you want to do a full backup of the items that you have selected or back up changes only? You can override this selection when you run or schedule the policy. If you select changes only, you can specify if you want the backup to be an incremental or cumulative backup.
Full backup
Changes only
Changes since last full backup (cumulative)
Changes since last backup (incremental)
Allow overrides to backup activity when policy is run or scheduled
Help
< Back
Next >
Finish
Cancel

Figure 6-17 Selecting full backup

12. You are now prompted for the initial mode of the backup. You will back up to a tape or virtual tape. Depending on your environment, other options are appropriate. For our example, select **Back up to media** and click **Next** (Figure 6-18).

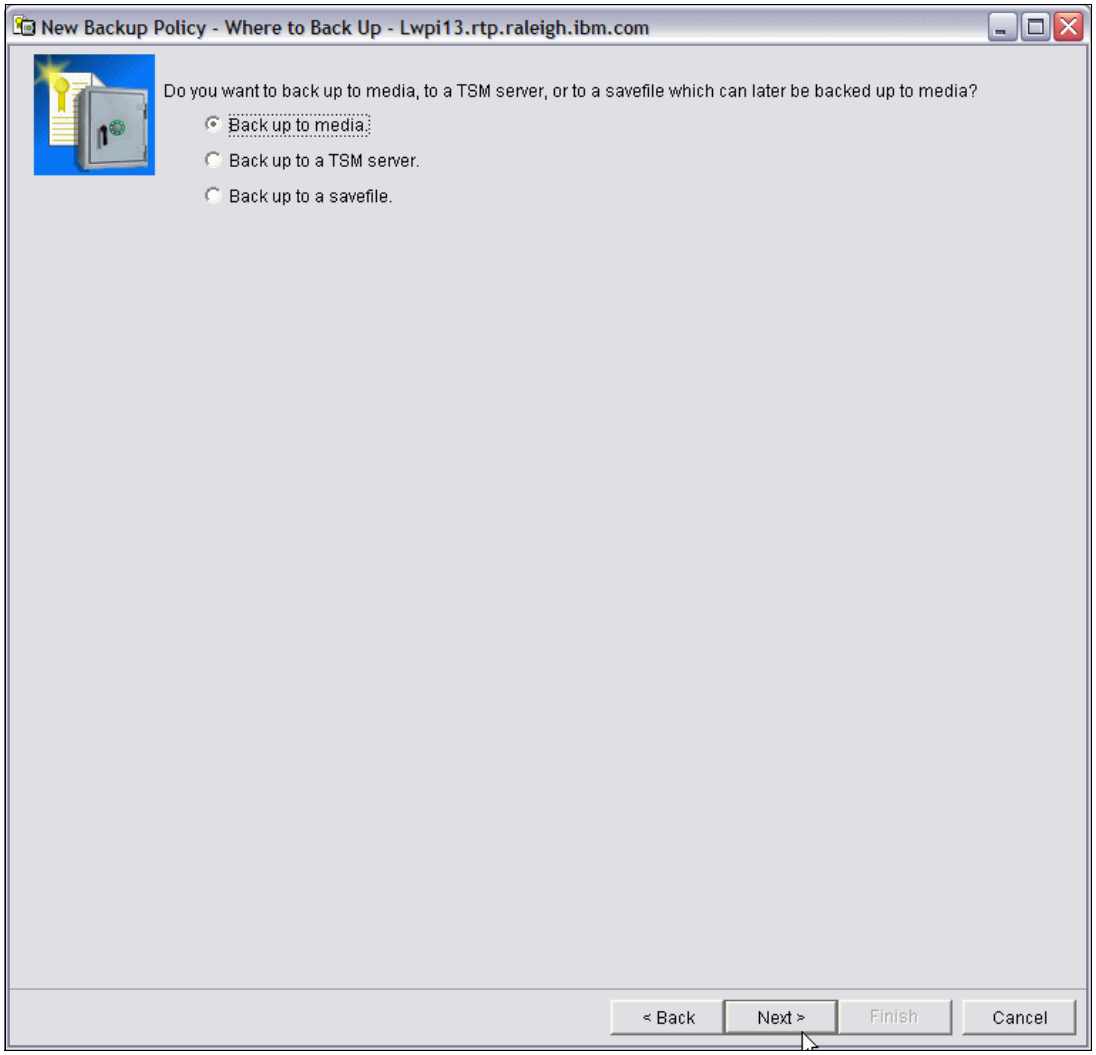

New Backup Policy - Where to Back Up - Lwpi13.rtp.raleigh.ibm.com
Do you want to back up to media, to a TSM server, or to a savefile which can later be backed up to media?
Back up to media.
Back up to a TSM server.
Back up to a savefile.
< Back
Next >
Finish
Cancel

Figure 6-18 Specifying the backup media

13. You can select the number of days to retain the information of the backup media (tape). Enter the number of days if you want to change it. Leave the default of 21 days for now (Figure 6-19). You can increase this number for your environment.

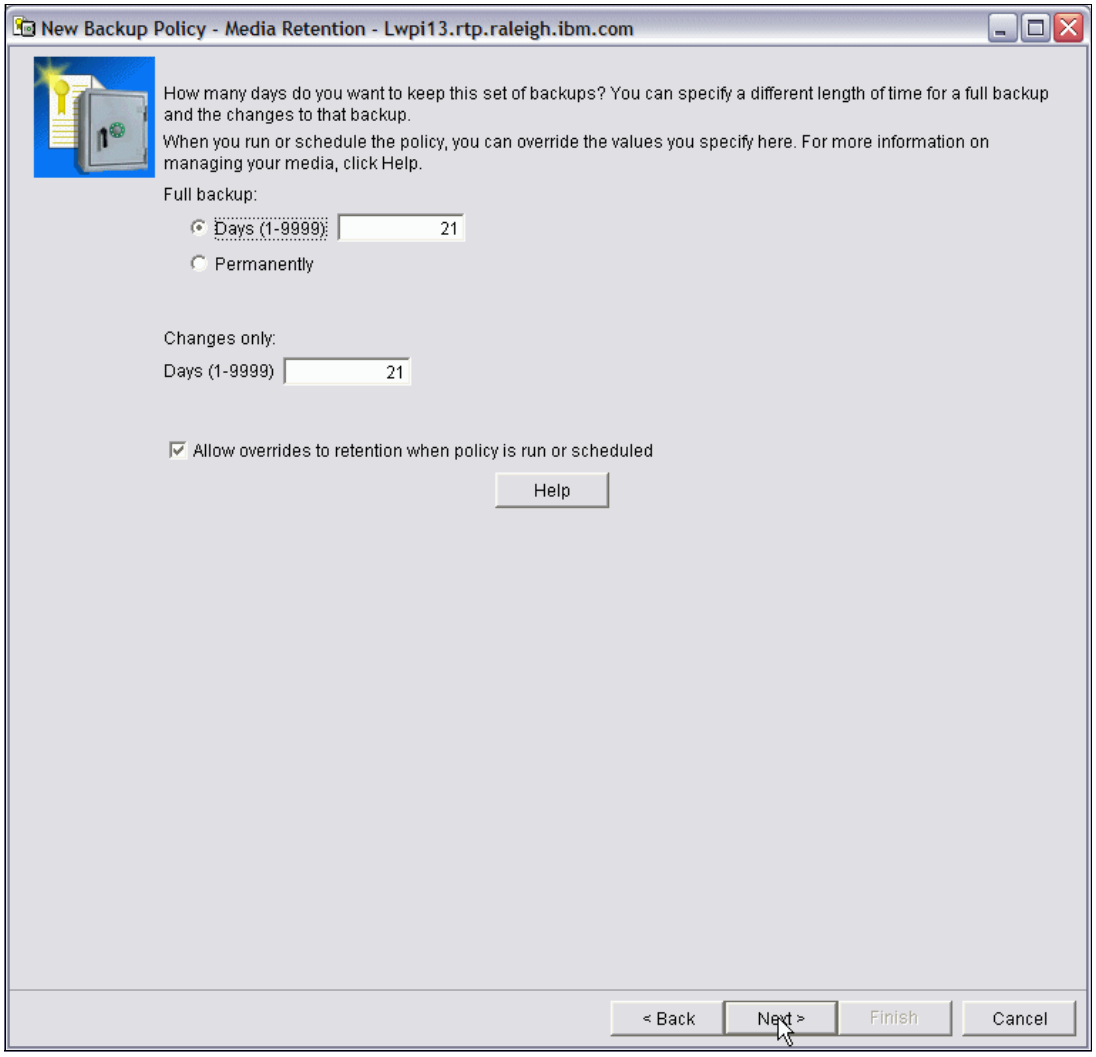

New Backup Policy - Media Retention - Lwpi13.rtp.raleigh.ibm.com
How many days do you want to keep this set of backups? You can specify a different length of time for a full backup and the changes to that backup.
When you run or schedule the policy, you can override the values you specify here. For more information on managing your media, click Help.
Full backup:
Days (1-9999)
21
Permanently
Changes only:
Days (1-9999)
21
Allow overrides to retention when policy is run or scheduled
Help
< Back
Next >
Finish
Cancel

Figure 6-19 Specifying the media backup

14. Choose the backup devices from the list. You need to know the different classes of media your backup device supports. In our example, we are using a default of `Tap01`. Our backup tapes are of class `SLR60` so we choose that media class. The drop-down list shows you all the various media classes that you have defined in your environment. Choose what applies to your environment and click **Next**. (Figure 6-20).

> **Tip:** In V5R4, we recommend using virtual tape, which might be very fast, and then back up to tape at a later time. You can also use other options, such as Tivoli Storage Manager servers. For more information about virtual tape, see the i5/OS Information Center at:
>
> `http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzam4/rzam4virtualtape.htm`

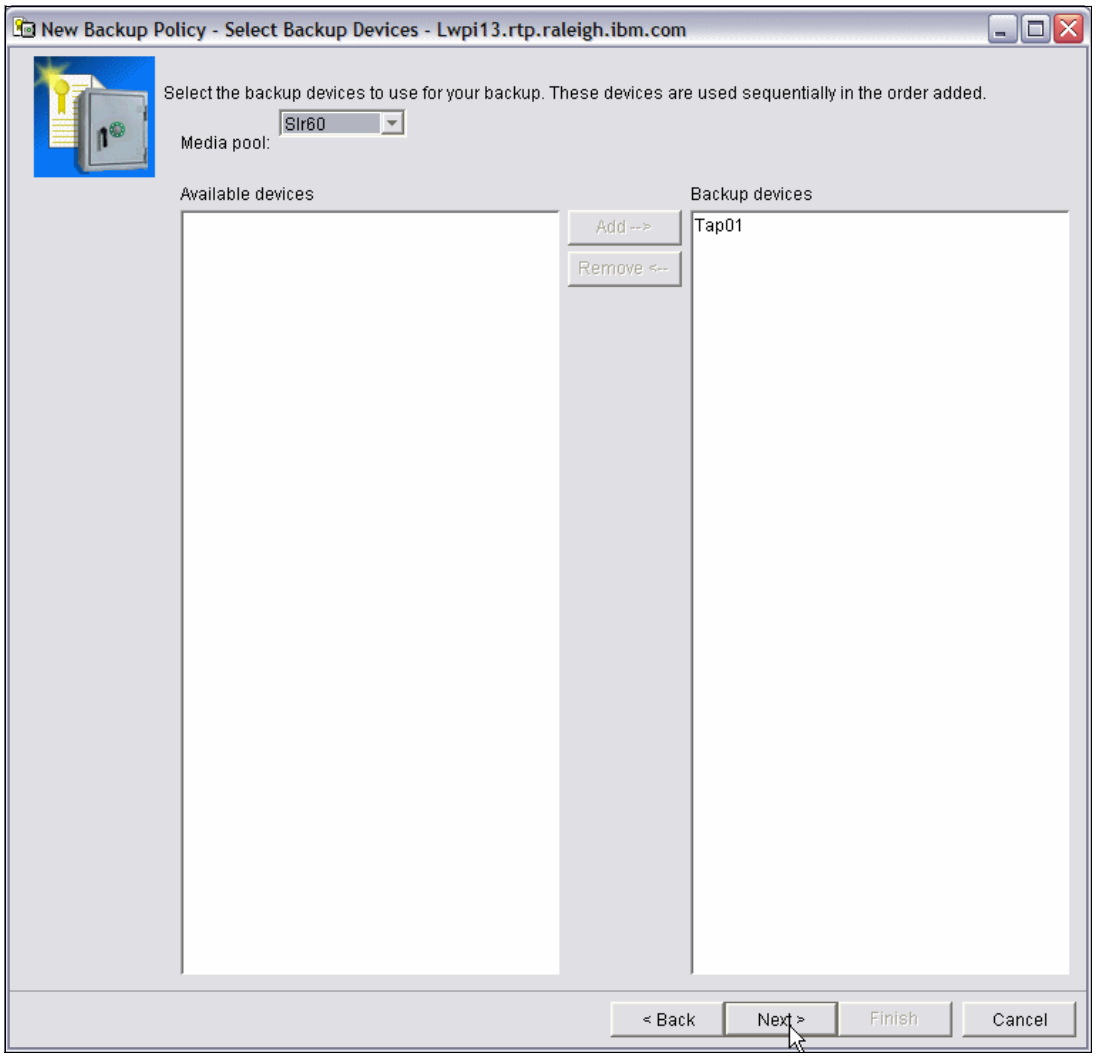


Figure 6-20 Selecting the backup device

15. You might decide to mark your media for duplication so another copy is made for storage at an external location. Select **Yes - mark the media for duplication (**Figure 6-21). Click **Next**.

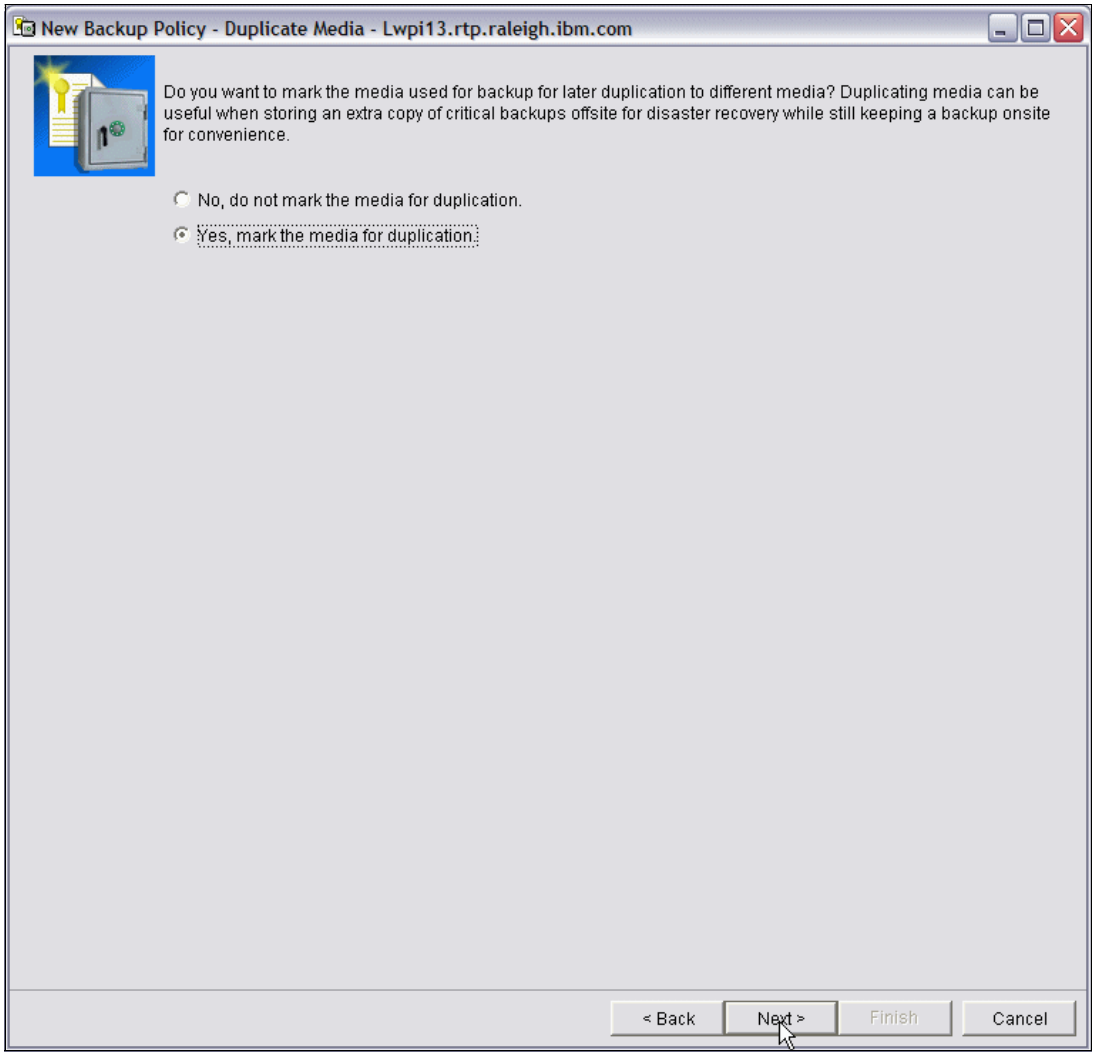

New Backup Policy - Duplicate Media - Lwpi13.rtp.raleigh.ibm.com
Do you want to mark the media used for backup for later duplication to different media? Duplicating media can be useful when storing an extra copy of critical backups offsite for disaster recovery while still keeping a backup onsite for convenience.
No, do not mark the media for duplication.
Yes, mark the media for duplication.
< Back
Next >
Finish
Cancel

Figure 6-21 Specifying to allow media duplication at a later time

16. On the Run Maintenance window, specify for maintenance (clean up, delete expired files, and so on). In our example, select **Yes, run maintenance after backup** and click **Next** (Figure 6-22). You can use **Maintenance Options** to customize the maintenance or clean up. The default maintenance is usually enough**.**

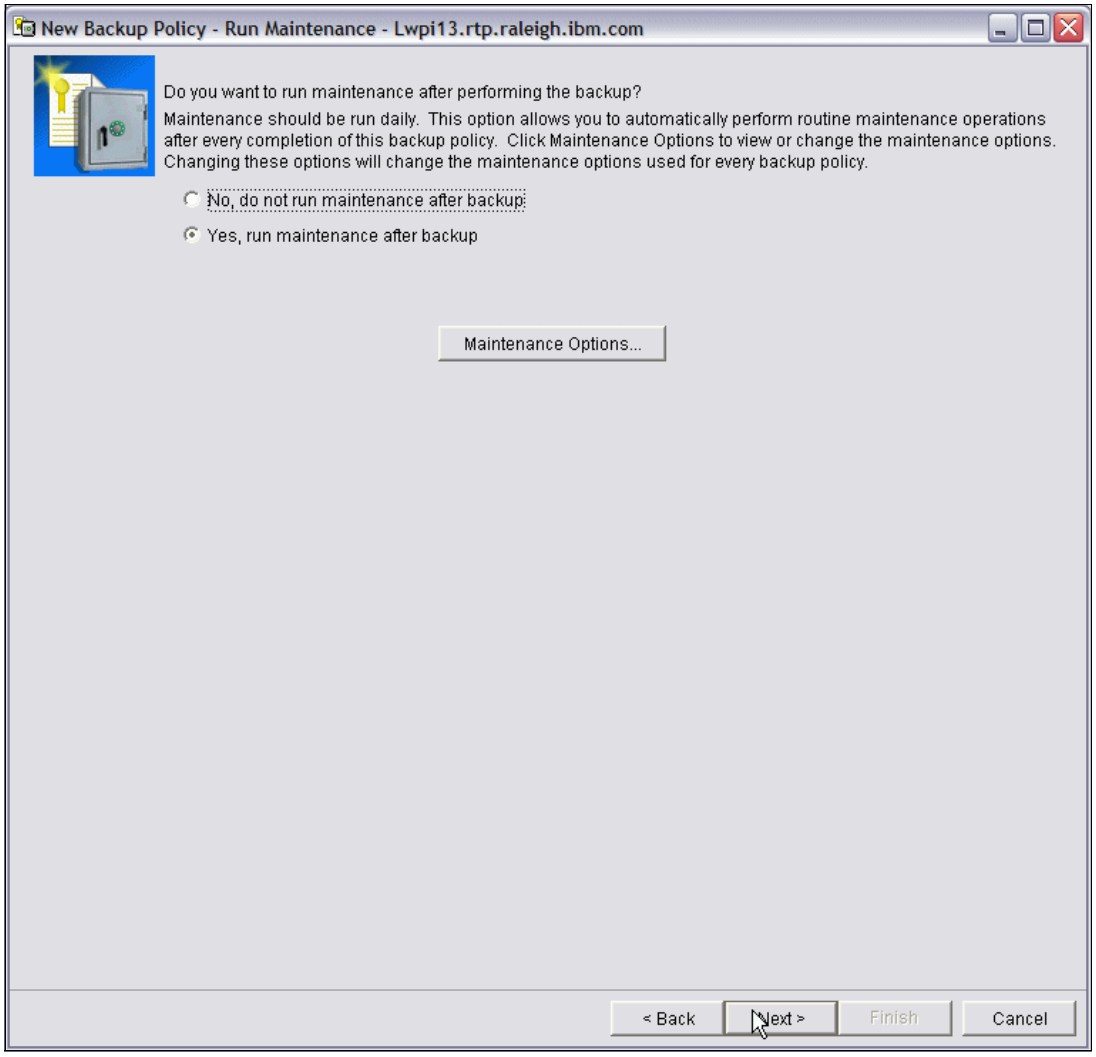

New Backup Policy - Run Maintenance - Lwpi13.rtp.raleigh.ibm.com
Do you want to run maintenance after performing the backup?
Maintenance should be run daily. This option allows you to automatically perform routine maintenance operations after every completion of this backup policy. Click Maintenance Options to view or change the maintenance options. Changing these options will change the maintenance options used for every backup policy.
No, do not run maintenance after backup
Yes, run maintenance after backup
Maintenance Options...
< Back
Next >
Finish
Cancel

Figure 6-22 Specifying basic maintenance

17. Next, you are prompted to add media devices. If you want to add any media, you are shown a few more windows concerning the tape or devices you want to add. After the backup policy is created, you also have the choice of adding volumes through the policy's properties panel. At this moment, do not add any media so select **No, the media is already added or I will add the media later** and click **Next** (Figure 6-23).

> **Tip:** You can use the Work with Media using the BRM (WRKMEDBRM) command to manage your media volumes.

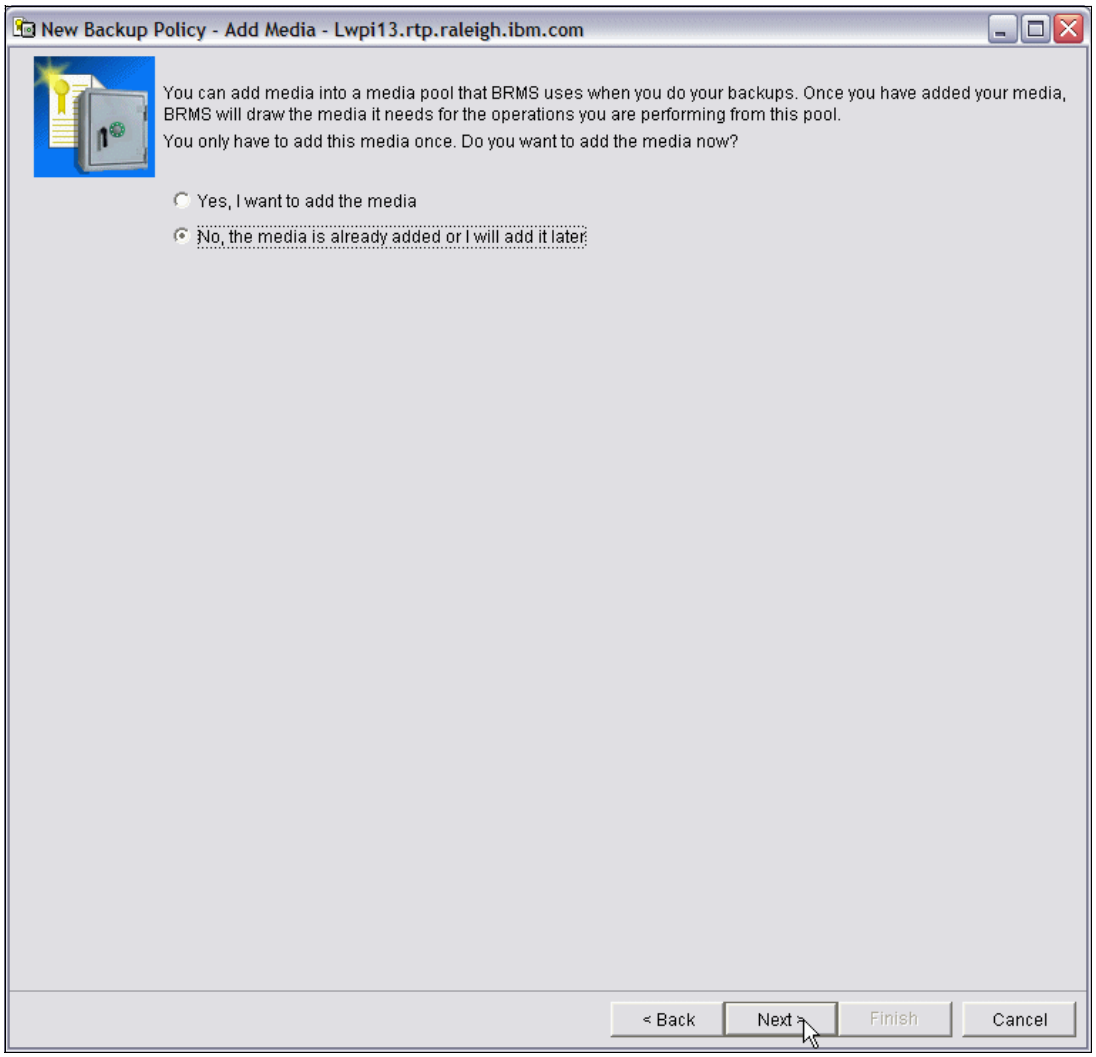

New Backup Policy - Add Media - Lwpi13.rtp.raleigh.ibm.com
You can add media into a media pool that BRMS uses when you do your backups. Once you have added your media, BRMS will draw the media it needs for the operations you are performing from this pool.
You only have to add this media once. Do you want to add the media now?
Yes, I want to add the media
No, the media is already added or I will add it later
< Back
Next >
Finish
Cancel

Figure 6-23 Specifying whether to add additional media

18. A summary window is shown. Click **Finish** (Figure 6-24).

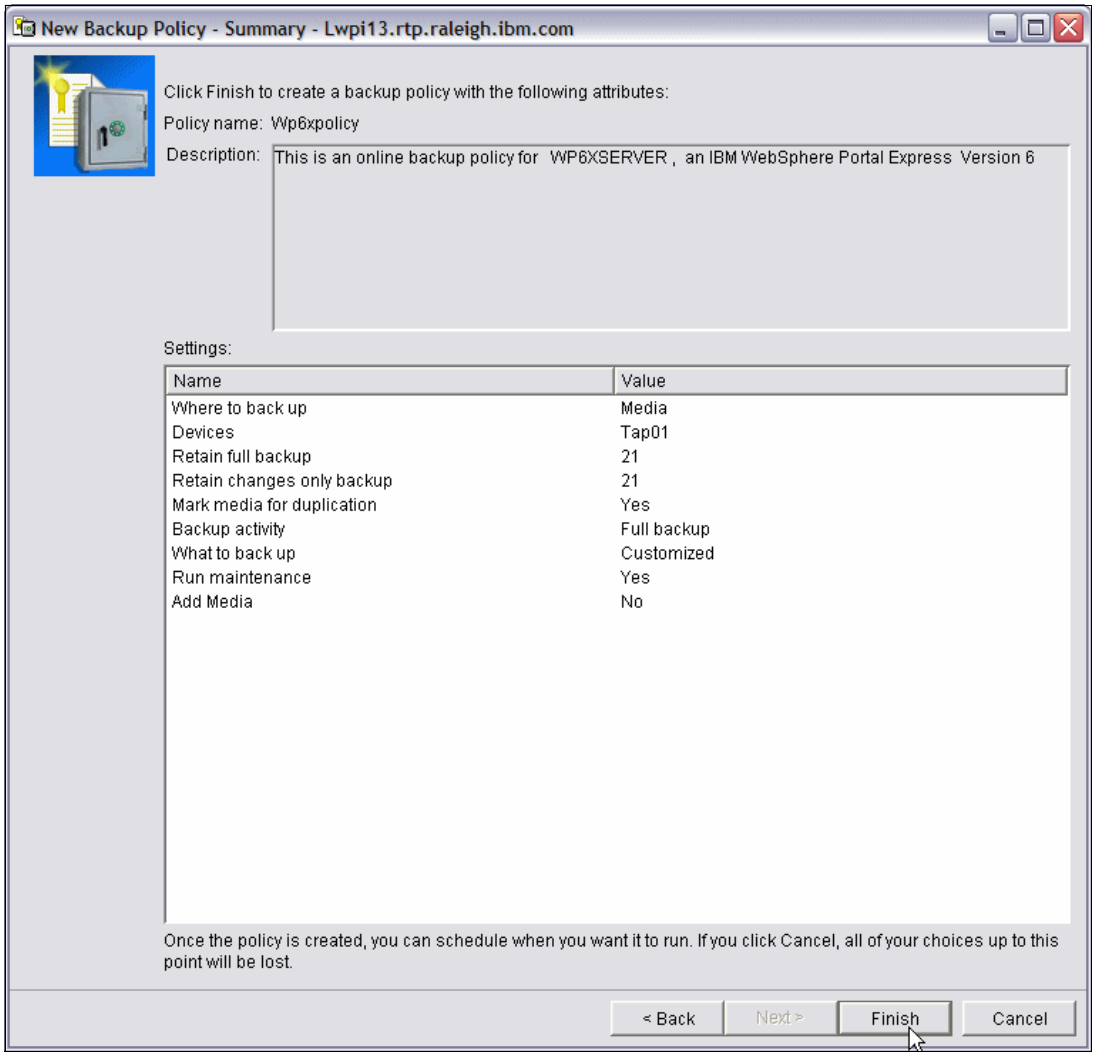


Figure 6-24 Reviewing Summary page

19. The New Policy wizard creates the defined lists and shows a Policy Created window. You can use this panel to schedule when this policy is run. For now, click **Done** (Figure 6-25).

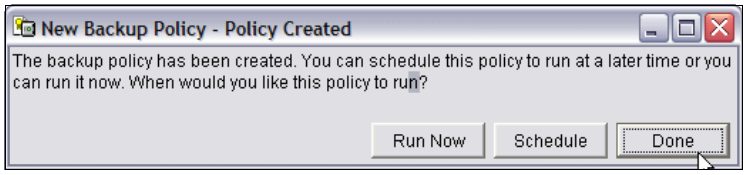

New Backup Policy - Policy Created
The backup policy has been created. You can schedule this policy to run at a later time or you can run it now. When would you like this policy to run?
Run Now
Schedule
Done

Figure 6-25 New backup policy created

Adding the directory and objects to omit from your backup

At this point, the backup policy is created. Next, use the policy's properties to add a list of objects that you want to omit from the online backup. This reduces the number of "objects in use" errors when you run the backup. Usually, you omit temporary files and logs that are not needed for the portal server to be functional. Perform the following steps:

1. From the iSeries Navigator, right-click the backup policy you just created and select **Properties**. In our example, this is `WP6XPOLICY` (Figure 6-26).

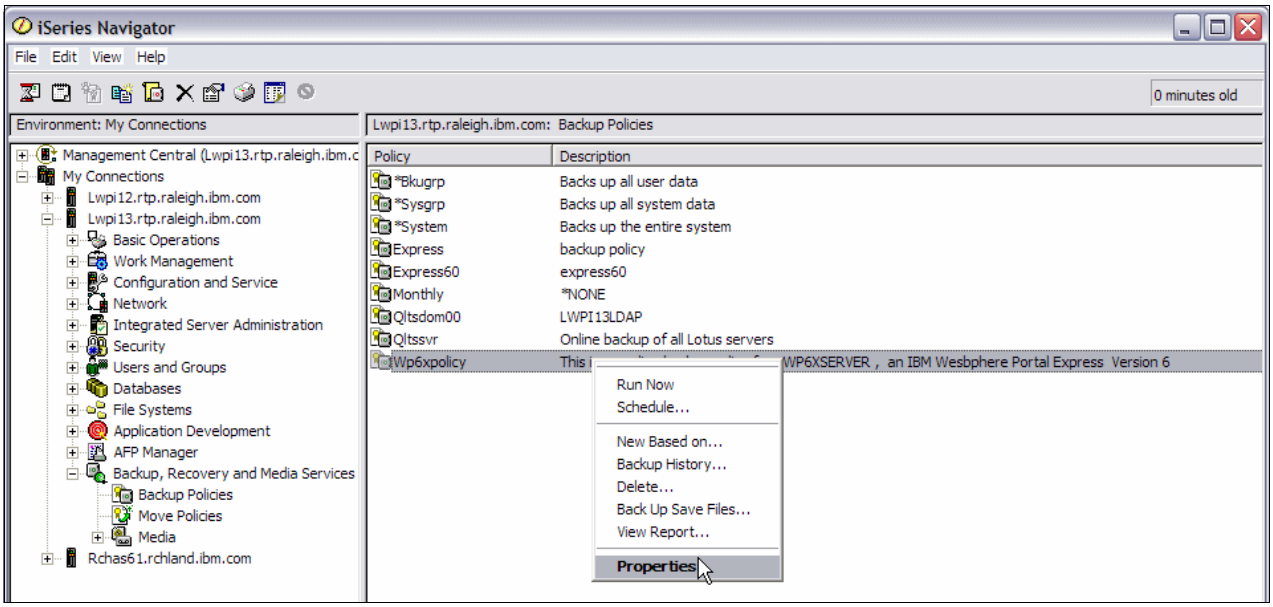


Figure 6-26 Selecting the backup policy's properties

2. On the backup policy Properties window, there are three boxes. These boxes allow you to specify what you can do before (pre-exit program), during, and after (post-exit programs) the backup. To add the omission lists or entries, you modify the activities used during the backup. Click the **During** box (Figure 6-27).

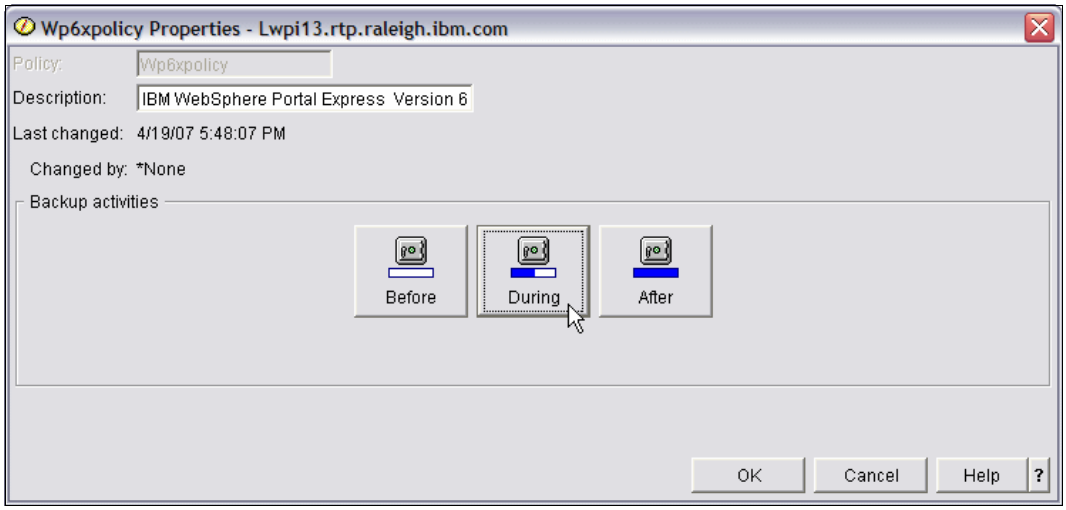


Figure 6-27 Backup policy properties

3. The During Backup window shows the list of items selected for the backup. The list shows libraries, directories, and objects. In our example, we want to add directories to omit. On the **What** tab, select the directory list of **wp6xpolicy** and click **Details** (Figure 6-28).

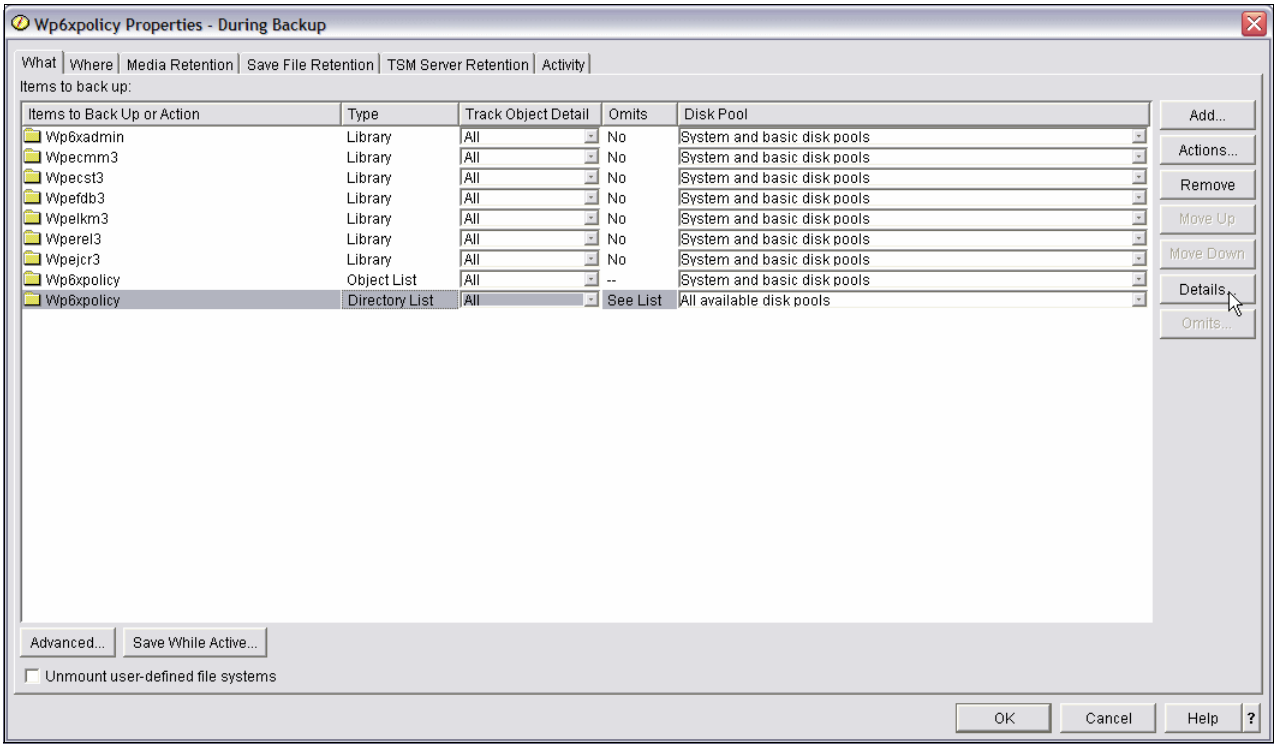


Figure 6-28 Selecting the directory list

4. In the next panel, we add all the folders and objects we want to omit. Our list is not exhaustive. It is a sample list. Ordinarily, you omit files that are in constant use and almost impossible to back up. These files usually include serialized files (*.ser), portal server logs, and temporary directories. Following are sample folders. Replace the list with what is appropriate in your environment. For our profile, `WP6XSERVER`, and the associated HTTP server, `WP6XWEB`, we want to omit the following entries:

```
/www/wp6xweb/logs/*
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/cache/*
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/temp/*
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/tranlog/*
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/wstemp/*
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/MarketWatch.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/logs/server1/nat
ive_StdErr.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/logs/server1/nat
ive_StdOut.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/logs/server1/Sys
temErr.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/logs/server1/Sys
temOut.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/log
/native_stderr.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/log
/native_stdout.log
```

```
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/log
/SystemErr.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/log
/SystemOut.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/log
/trace.log
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/logs/IHS_LWPI13_
WP6XWEB/http_plugin.log
```

For each of the directories listed above, fill in the value for **Directory or file path** and click **Add.** Then, select the check box next to the directory and under the Omit column**.** See Figure 6-29. Notice also that at the bottom of the window, the Include option is set to **All directories and subdirectories.** Click **OK** when you are done.

Note: The list of entries that is omitted is not exhaustive. You might need to add more files to it or reduce the number of files omitted. For example, if you are not using an external HTTP server, then the entries relating to them are not relevant in your environment. Always check the job log to inspect the files that were in use. If you decide that you need to back up certain files that were not backed up (such as these omitted entries), you can devise a way to make copies of those files and save them at a later time.

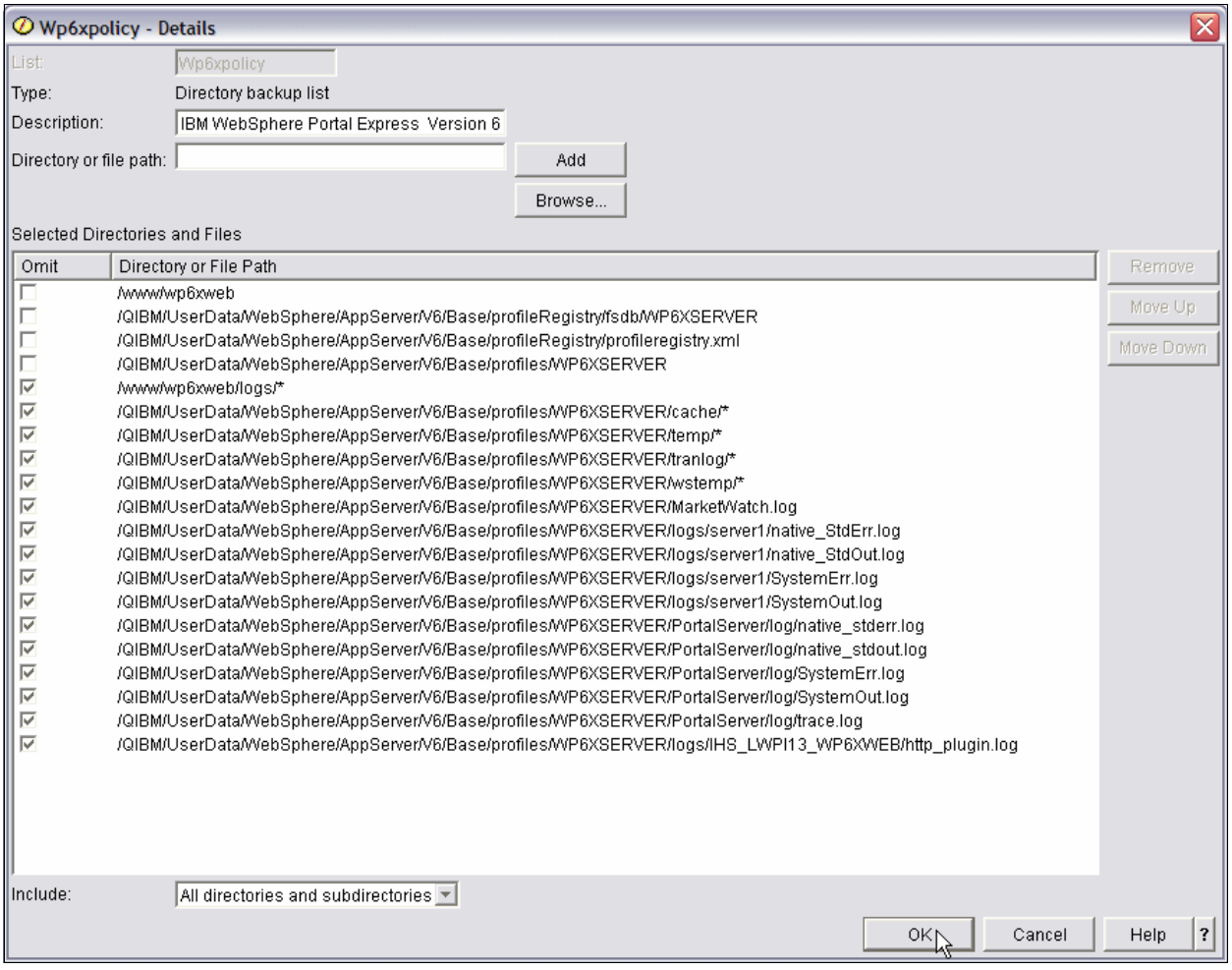


Figure 6-29 Omitting directories and files from the backup policy

5. The During Backup window is displayed again. Because you are doing an online backup, implement the Save While Active feature for the libraries and directories to be saved. Click **Save While Active** at the bottom of the page (Figure 6-30).

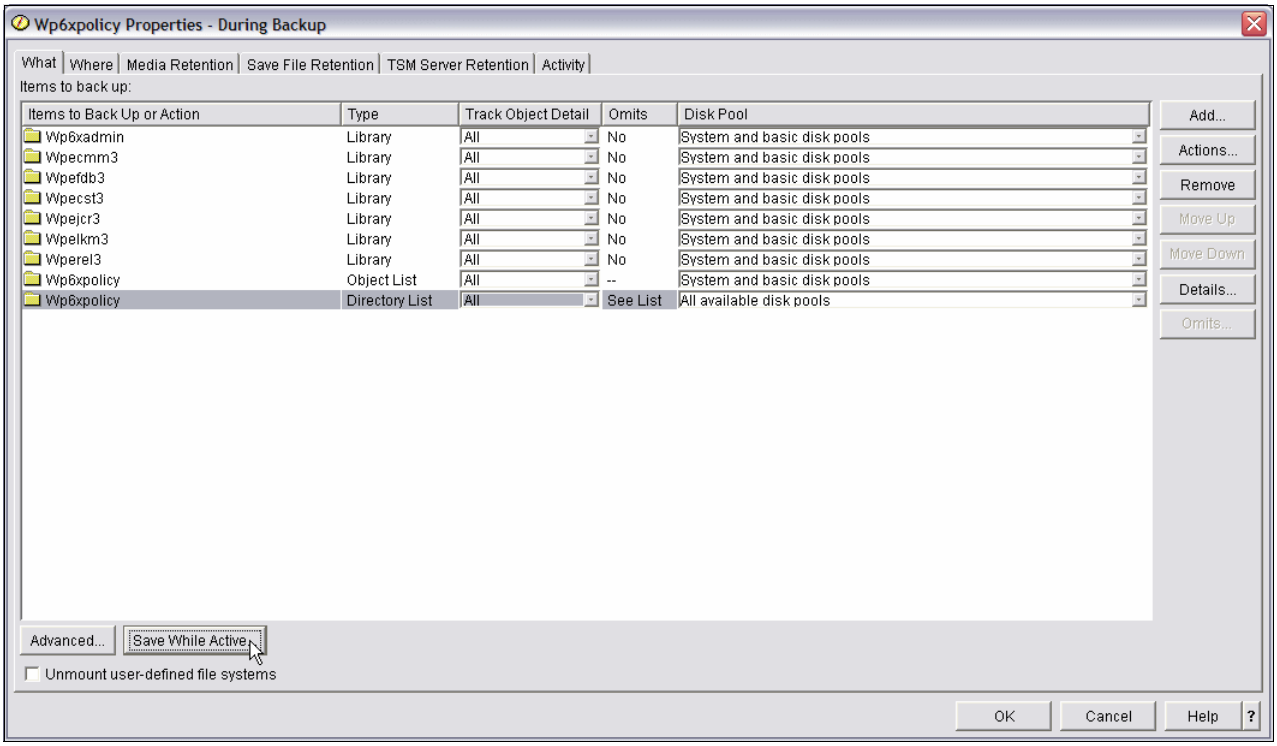


Figure 6-30 Accessing the Save While Active panel

6. On the Save While Active window, under the Save While Active column, click the drop-down icon to see the various options for the Save While Active activity (Figure 6-31). Perform the following steps to select the option for Save While Active for the various lists:

   a. For all the items of type Library, select the Save While Active option of **All libraries**.

   b. For Wp6xpolicy type of Object List, select Save While Active option of **No**.

   c. For Wp6xpolicy type of Directory List, select the Save While Active option of **Yes**.

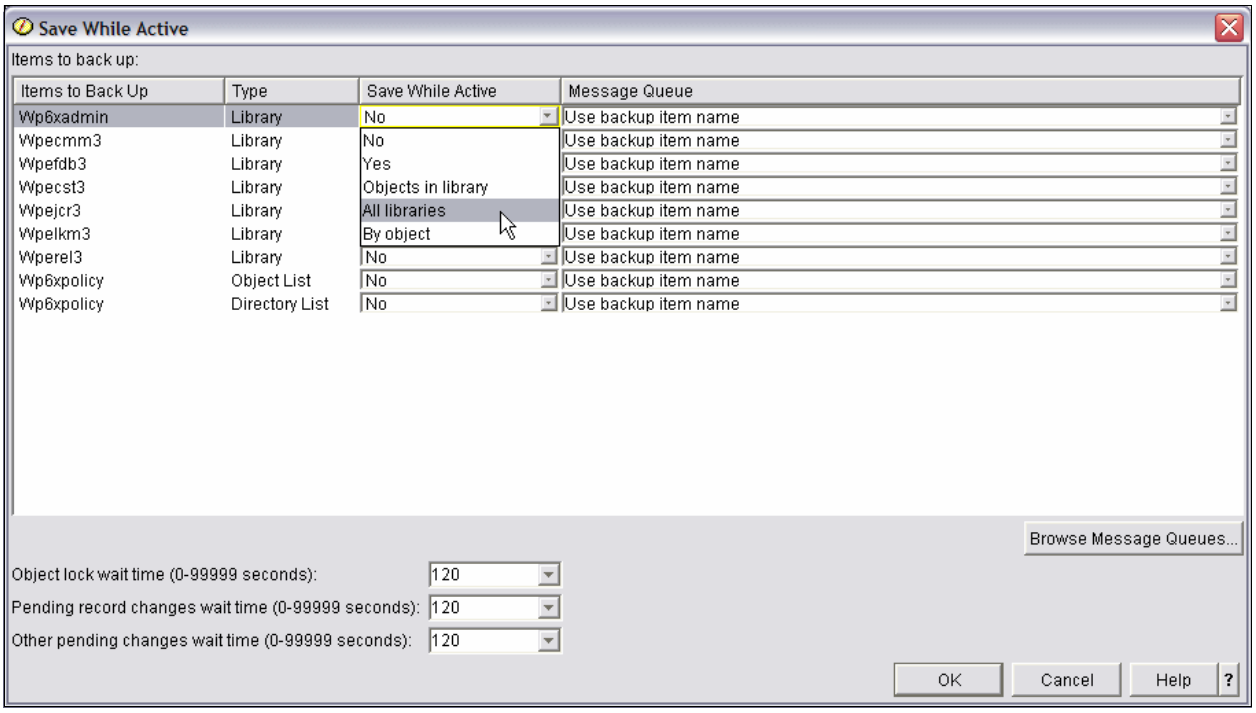


Figure 6-31 Specifying the Save While Active options

7. Figure 6-32 shows the list after completing the selections.

Important: You must specify **No** in the Save While Active column for the object in QUSRSYS/QATMHINSTC. The following statement is from the *Save-while-active restrictions* article in the i5/OS Information Center at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzaiu/rzaiurzaiu314.htm

If you have specified *NOCMTBDY for the SAVACTWAIT parameter, you cannot save any IBM library or any library that begins with Q (except for QGPL).

You are only saving a member in the QUSRSYS/QATMHINSTC file. The file does not change once it is created.

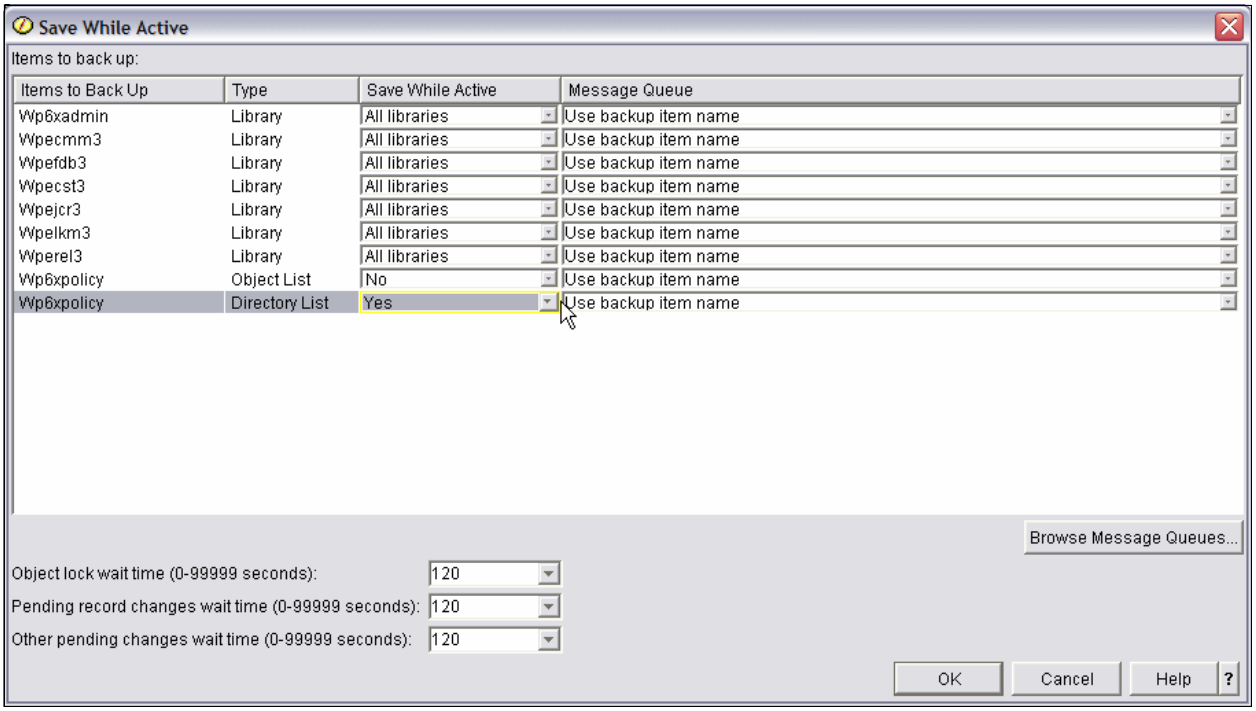

Save While Active
Items to back up:
Items to Back Up
Type
Save While Active
Message Queue
Wp6xadmin Library All libraries Use backup item name
Wpecmm3 Library All libraries Use backup item name
Wpefdb3 Library All libraries Use backup item name
Wpecst3 Library All libraries Use backup item name
Wpejcr3 Library All libraries Use backup item name
Wpelkm3 Library All libraries Use backup item name
Wperel3 Library All libraries Use backup item name
Wp6xpolicy Object List No Use backup item name
Wp6xpolicy Directory List Yes Use backup item name
Browse Message Queues...
Object lock wait time (0-99999 seconds): 120
Pending record changes wait time (0-99999 seconds): 120
Other pending changes wait time (0-99999 seconds): 120
OK
Cancel
Help
?

Figure 6-32 Save While Active options selected

8. At the bottom left of the Save While Active window, there are three options on wait times for the various kinds of transactions. For our example, we want to use open commit cycles so that when objects are saved, we save them immediately without waiting for incomplete transactions on the object to reach a commitment boundary or roll back. We are saving the object in a ragged state. To do this, select the drop-down list next to Pending record changes wait time (0-99999 seconds) and select **No Wait Time**. Use **Help** for more information. Click **OK** to continue (Figure 6-33).

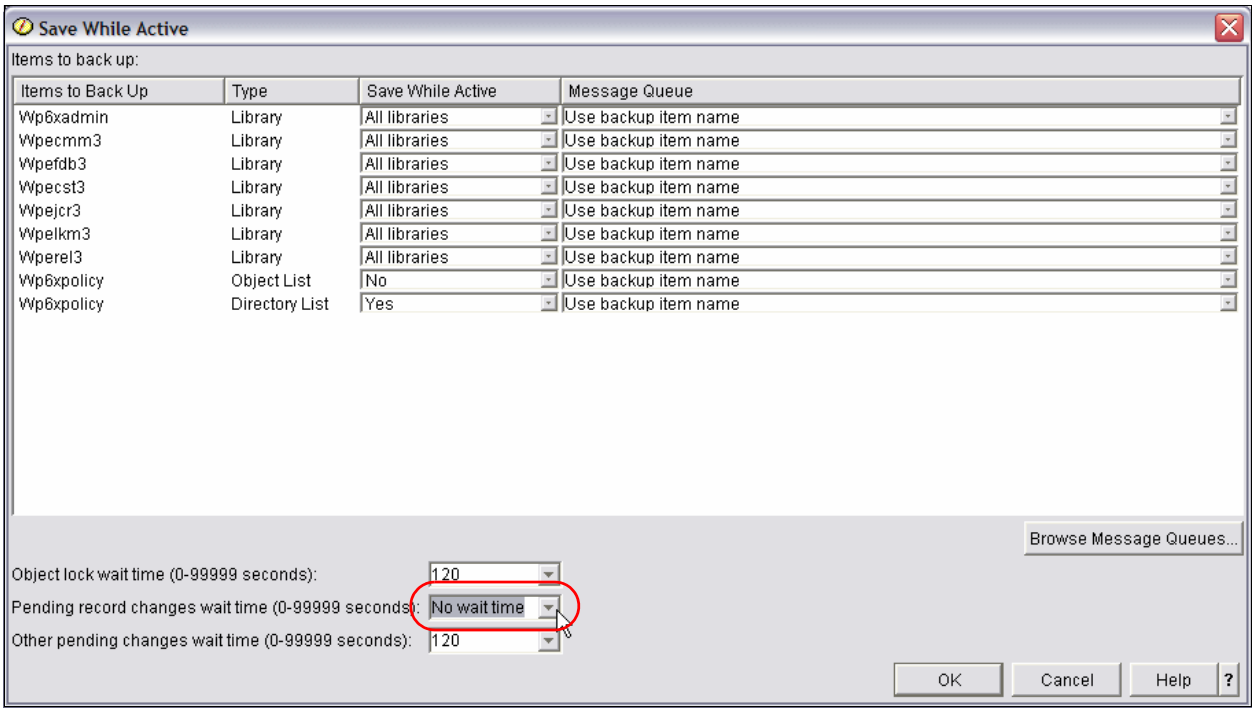


Figure 6-33 Specifying ragged saves

9. You have been working on the What tab, next access the Activity tab to customize your saves. Click the **Activity** tab on the far right**.** On this tab, notice that the default choice for the Type of changes only backup is **Changes since last full backup (cumulative).** This is what you want for the changes only portion of your save**.** The Type of changes only backup choice only works if the saves are changes only, or you are using a customized backup that includes a combination of full backup and changes only. For our example, select the **Customized** radio button and click **Customize** (Figure 6-34).

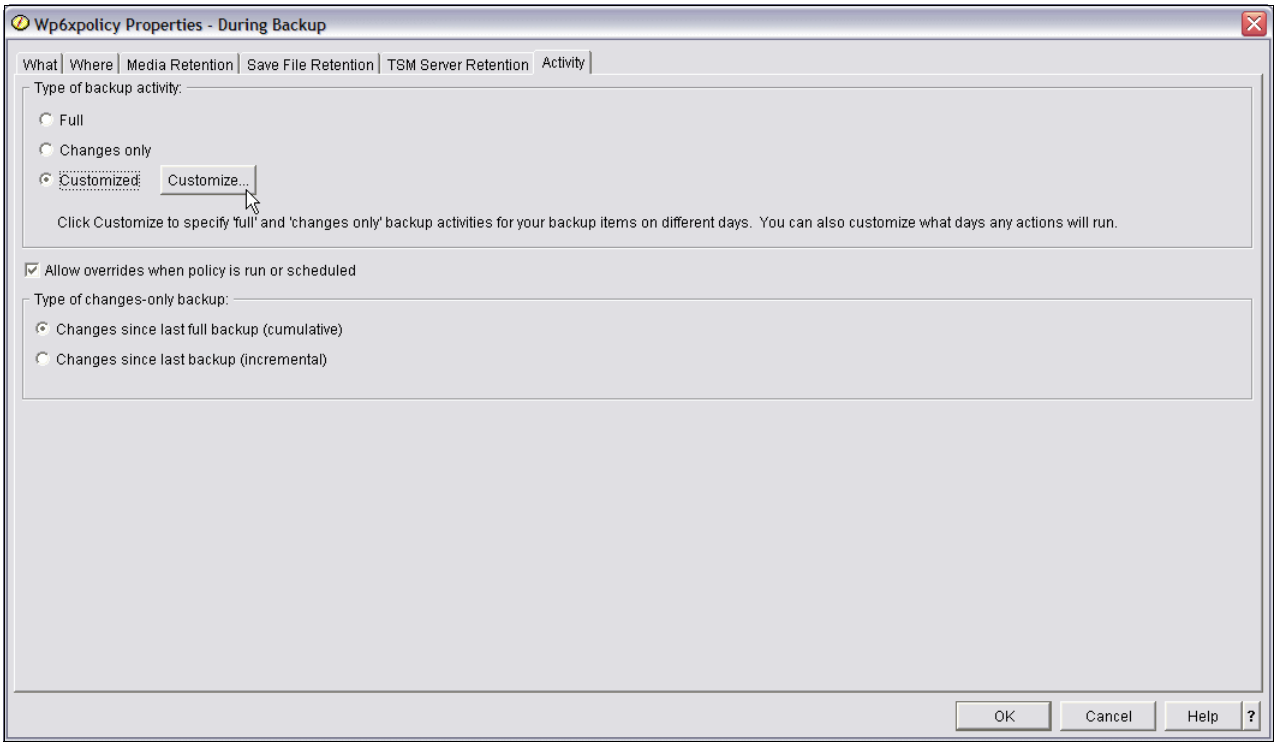


Figure 6-34 Selecting the customized type of backup activity

10. The Customize window defines the nature of the saves. For our example, you want full backups everyday for the library and objects, full backup on one day of the week (Sunday) for stream files, and cumulative changes (changes since Sunday) for stream files for each of the remaining days of the week:
    - To select full backups for libraries, click the check boxes for each of the libraries in every column.
    - To select full backups for the object list, click the check boxes for the Object List type so that there is a check in a white or clear background for every column
    - To select full backups for the stream files, click the check box for the Directory List type in the **Sunday** column so there is a check in a white or clear background.
    - To select changes only backup for the stream files for the rest of the week, check the check boxes for **Directory List** type so there is a check in a slightly darkened box in every other column for the rest of the week (Monday through Saturday).

    The selections are obvious for full backup as compared to changes for only backup. An example window after the selections are made is shown in Figure 6-35. Click **OK** after inspecting your selections.

> **Note:** This is how the save will work. Assume the first save you do is on a Tuesday. The policy indicates changes only for Tuesday. However, because this is the first save, changes only will include all data, hence a full backup for that day. Apart from the first save, subsequent saves will follow the format you have.

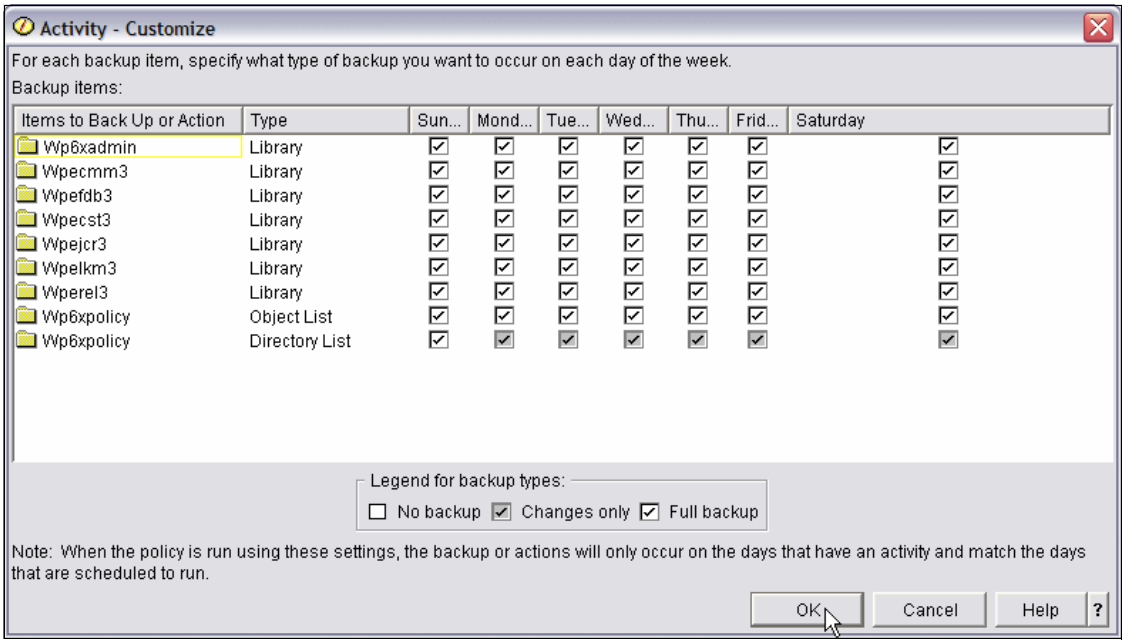


Figure 6-35 Implementing full and cumulative changes

11. You are returned to the Activity tab. Click **OK** to continue (Figure 6-36).

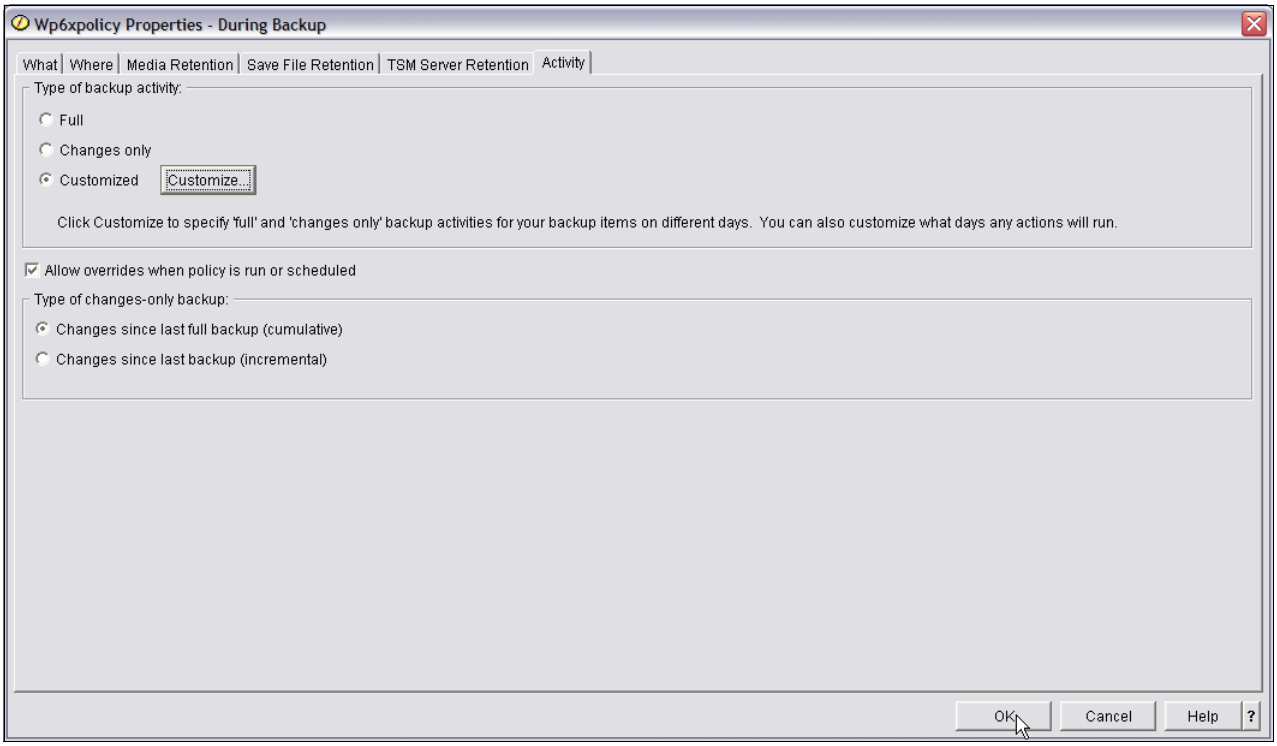


Figure 6-36 Clicking OK to continue

Saving security data, user profiles, and object authorities

At this moment, the integrated file system object authorities are not saved with the object when the object is saved. This poses a problem when you restore the objects. For example, QTMHHTTP and QEJBSVR profiles need specific access to certain files (private authorities) for the external HTTP server and the WebSphere Portal Express V6 server to function properly. More importantly, the concept of profiles in portal requires a unique Database Administrator owner for every profile. In essence, you need to save these necessary private authorities and the user profile. There is no easy way to save the Database Administrator user profile so save all security data, including all user profiles.

You can use the ExpressSave.sh script to create and store authorities and security data. Specifically, the save file USERPROFS is created in the library QGPL and, when selected for backup, stores the output of the Save Security Data (SAVSECDTA) CL command. Other stream files are created to store the authorities of the profile and saves as data with the backup.

Perform the following steps to set up the backup policy information:

1. From the backup policy Properties window, click **Before** to set up the ExpressSave.sh script so it is run before the actual save is kicked off (Figure 6-37 on page 283).

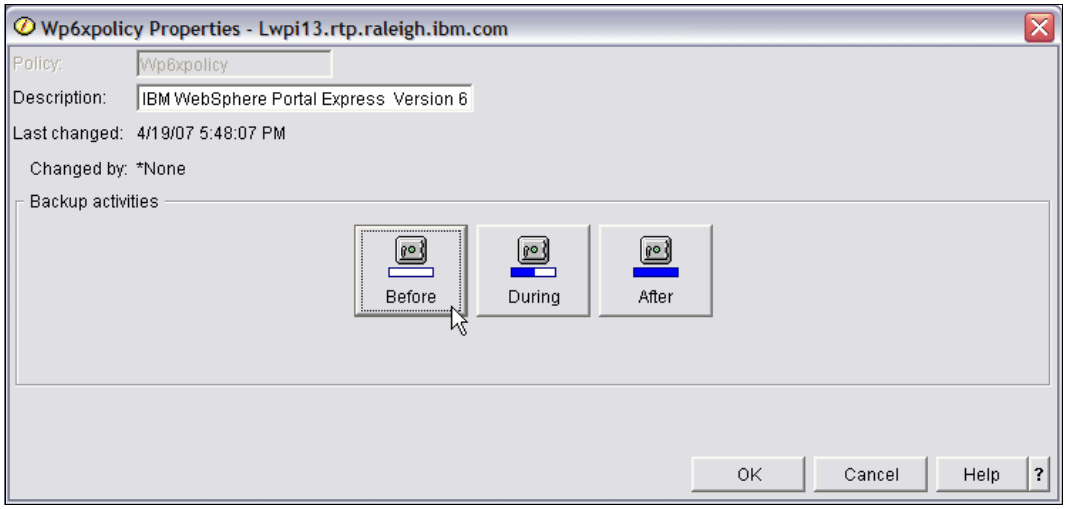


Figure 6-37 Backup policy properties

2. On the Before Backup window (Figure 6-38), enter the following values:
   a. In the Command to run field, enter the following command. In our example, replace <*profilename*> with WP6XSERVER:

      ```
      STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/ExpressSave.sh -p
      <profilename>')
      ```

   b. In the Days to run section, select all the days of the week**.** This is because we want to collect the private authorities for objects every time we save. The script takes a few minutes to run.
   c. Deselect **Shut down integrated server.** Click **OK**.

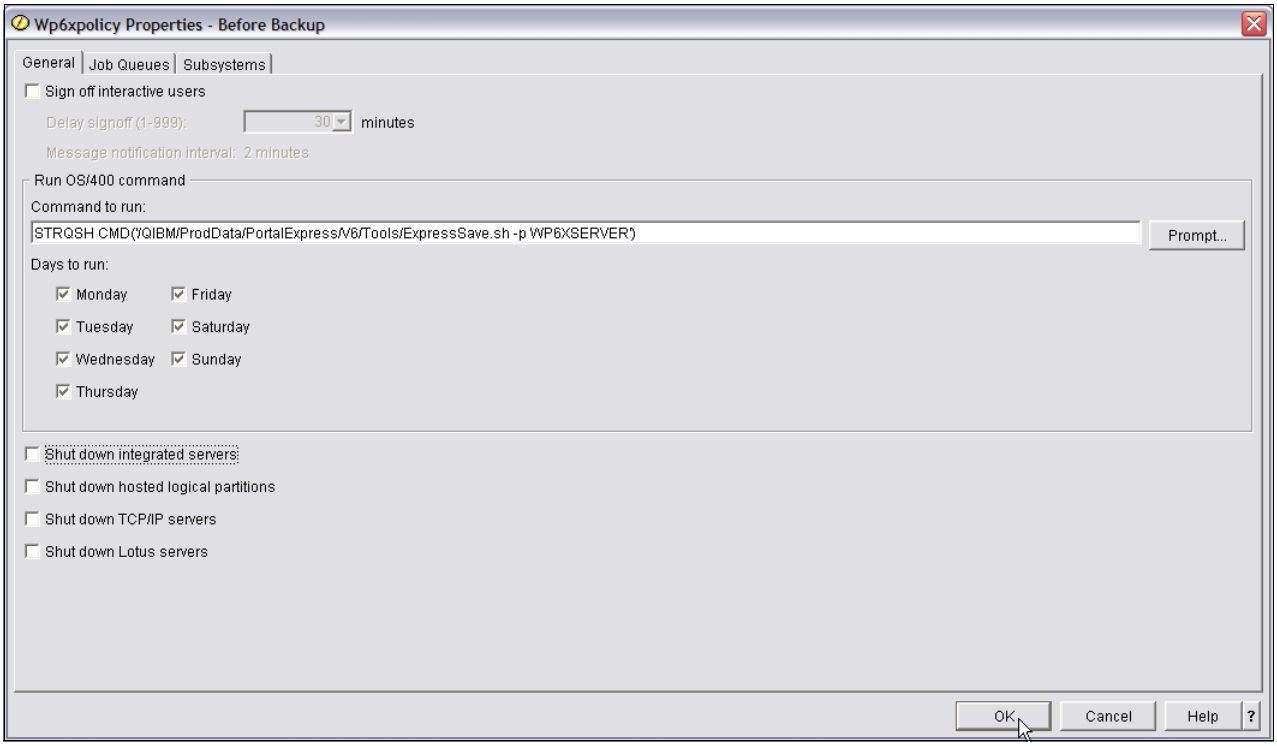


Figure 6-38 Specifying the before backup policy information

3. Because you created and stored the QGPL/USERPROFS save file with the backup, clear the save file's content after the backup is complete. Click **After** to access post-backup processing (Figure 6-39).

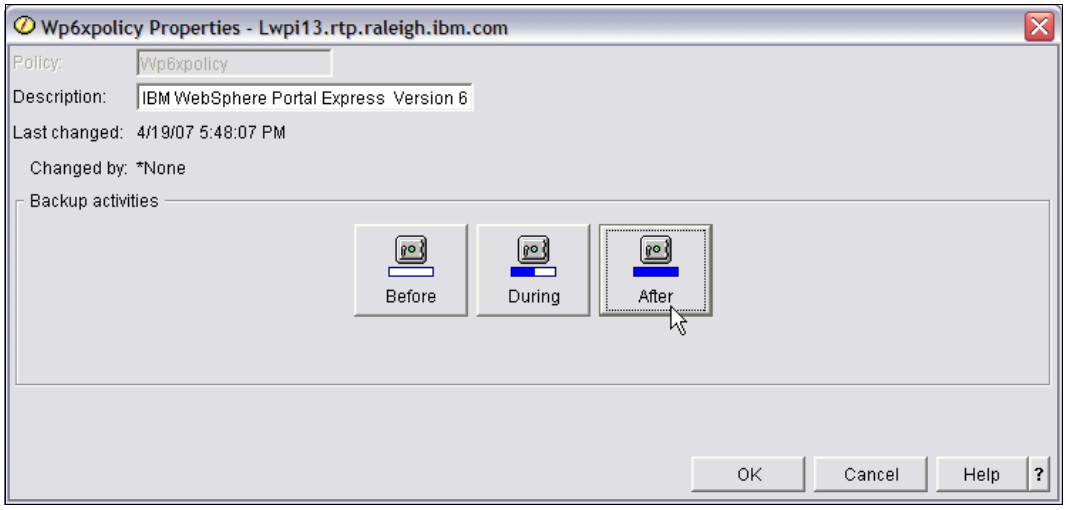


Figure 6-39 Using After to clean up

4. On the After Backup window (Figure 6-40), enter the following command in the Run OS/400 command field:

   ```
   CLRSAVF FILE(QGPL/USERPROFS)
   ```

   Click **OK.**

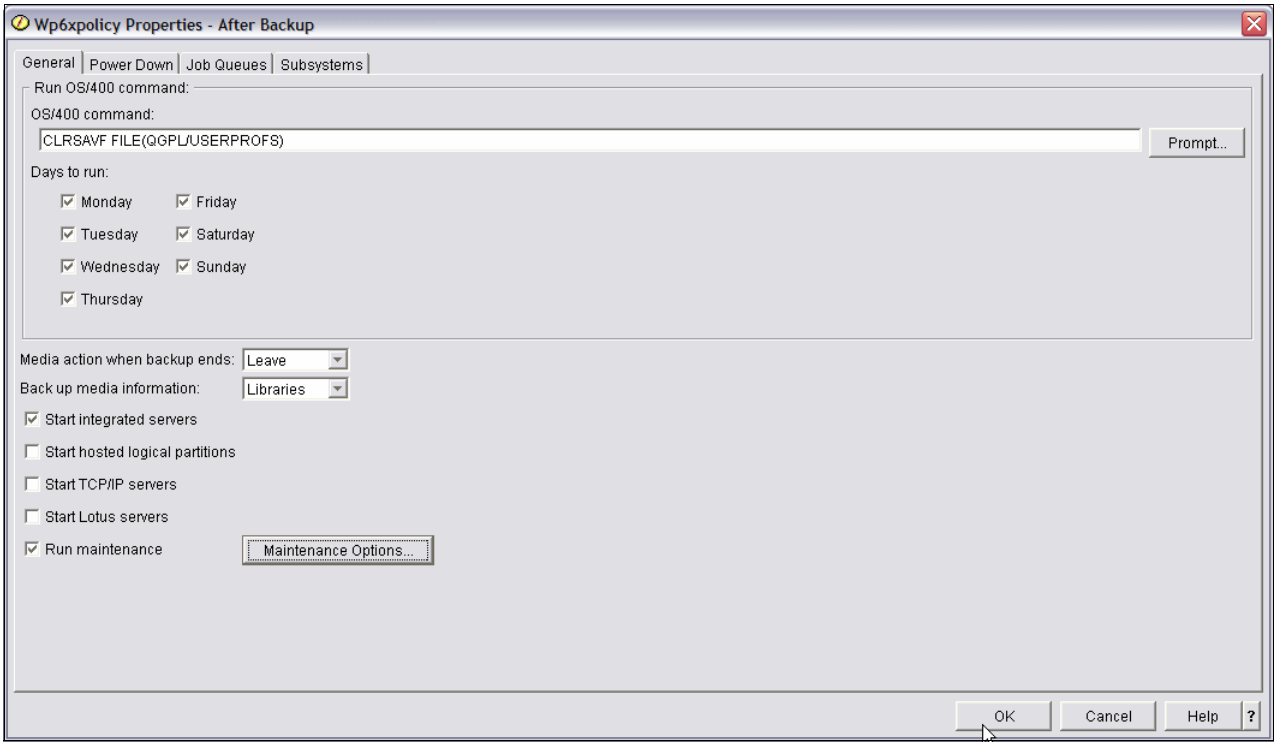


Figure 6-40 Specifying the after backup policy information

5. Click **OK** to exit the backup policy's Properties window (Figure 6-41).

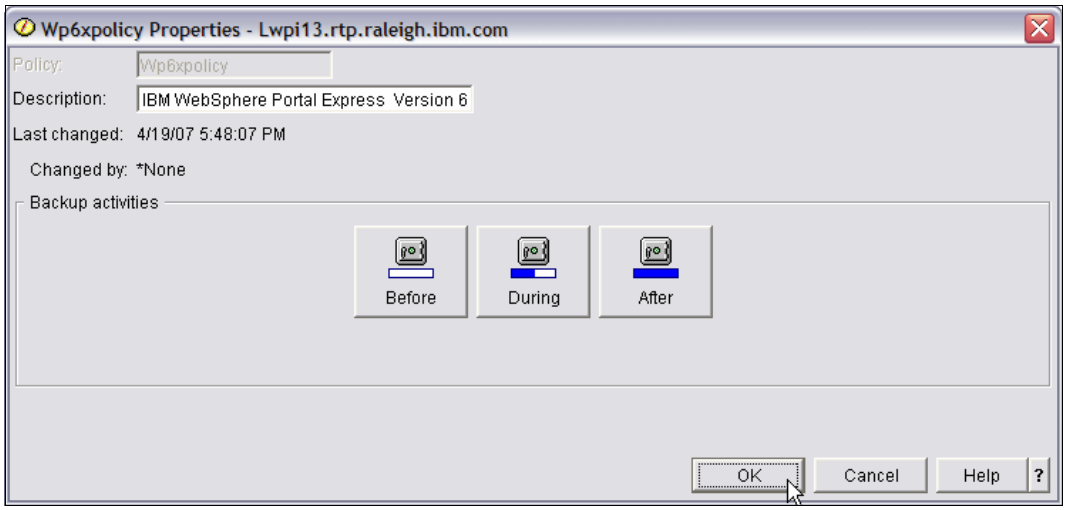


Figure 6-41 Clicking OK to exit the backup policy's properties window

6. You are now done setting up the backup policy.
7. Figure 6-42 shows how the backup policy looks in a 5250 emulation session after entering the Work with Backup Control Groups (WRKCTLGBRM) command and then typing option 5 to display it.

```
                  Display Backup Control Group Entries              LWPI13

 Group..........: WP6XPOLICY
 Default activity....:
 Text..........: This is an online backup policy for   WP6XSERVER,

                       Auxiliary   Weekly    Retain  Save      SWA
      Backup      List  Storage     Activity  Object  While     Message
 Seq  Items       Type  Pool Device SMTWTFS   Detail  Active    Queue
   10  *EXIT                       *******
   20  WP6XADMIN         *SYSBAS     FFFFFFF   *YES    *SYNCLIB  *LIB
   30  WPECMM3           *SYSBAS     FFFFFFF   *YES    *SYNCLIB  *LIB
   40  WPEFDB3           *SYSBAS     FFFFFFF   *YES    *SYNCLIB  *LIB
   50  WPECST3           *SYSBAS     FFFFFFF   *YES    *SYNCLIB  *LIB
   60  WPEJCR3           *SYSBAS     FFFFFFF   *YES    *SYNCLIB  *LIB
   70  WPELKM3           *SYSBAS     FFFFFFF   *YES    *SYNCLIB  *LIB
   80  WPEREL3           *SYSBAS     FFFFFFF   *YES    *SYNCLIB  *LIB
   90  WP6XPOLICY  *OBJ  *SYSBAS     FFFFFFF   *YES    *NO
  100  WP6XPOLICY  *LNK  *ALLAVL     FIIIIII   *YES    *YES      *LIB
 110 *EXIT            *******
Press Enter to continue.

 F3=Exit   F11=Display exits   F12=Cancel   F14=Display client omit status
```

Figure 6-42 Displaying the backup policy from a 5250 emulation session

6.3.2 Scheduling your backup with the advanced job scheduler

This section describes the process of scheduling your backup using the advanced job scheduler. Perform the following steps:

1. From the iSeries Navigator, expand **Backup, Recovery and Media Services,** click **Backup Policies,** right-click **WP6XPOLICY,** and select **Schedule** (Figure 6-43).

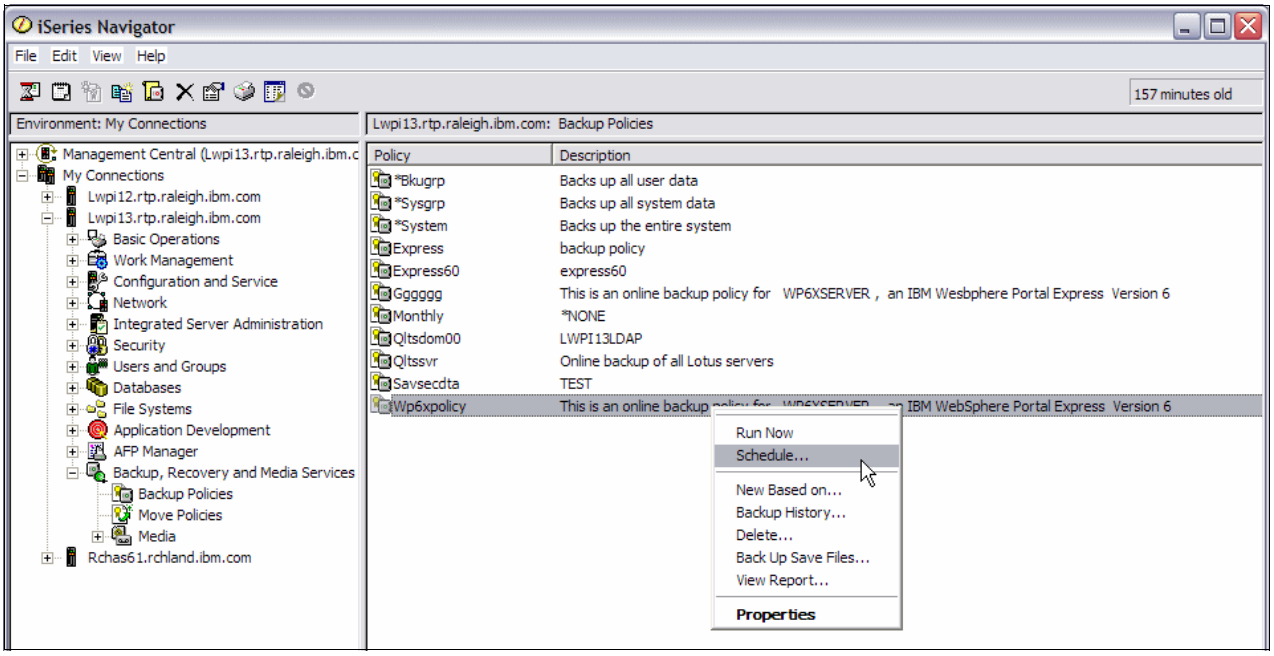


Figure 6-43 Scheduling the backup job

2. On the Run Backup Policy window, keep the default of **Use policy setting - Customized.** Click **OK** (Figure 6-44).

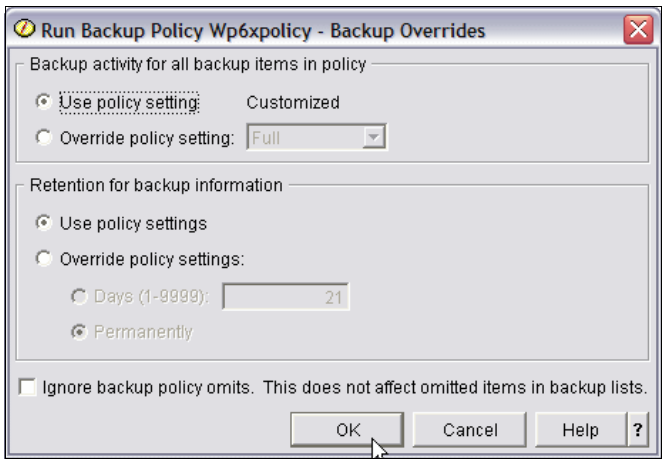


Figure 6-44 Scheduling the customized policy

3. A connection is made to the Management Central system at this point. If the connection fails, you need to fix the Management Central connection issue and restart the schedule process.

4. The Management Central Scheduler is shown. In the When to run section, select **Daily.** In the Time to start section, enter a time. For our example, we enter `9:00:00 PM`. Click **OK** (Figure 6-45).

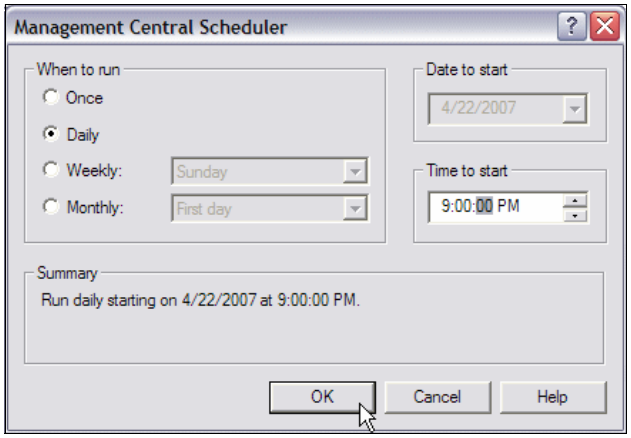


Figure 6-45 Specifying schedule specific information

5. You are then notified the job has been scheduled as shown in Figure 6-46. Click **OK**.

iSeries Navigator
Task 'Run 'Wp6xpolicy' backup policy (20)' has been scheduled. Look in Scheduled Tasks under Management Central to view status and work with this task.
Show this message again
OK

Figure 6-46 Task has been scheduled

At this point, a job using a customized backup plan is scheduled to run at 9:00PM daily.

6.3.3 Running an online backup of the WebSphere Portal Express V6 server

In this example, we run the backup using the newly created backup policy, `wp6xpolicy`.

See the *BRMS iSeries Navigator Client Student Guide* to ensure that you have added your media to the BRMS volume and that the device is mounted. You can use the Work with Media using BRM (WRKMEDBRM) command to access the interface through which you can add the volume.

Perform the following steps:

1. From the iSeries Navigator, expand **Backup, Recovery and Media Services,** click **Backup Policies,** right-click **wp6xpolicy**, and select **Run Now** (Figure 6-47).

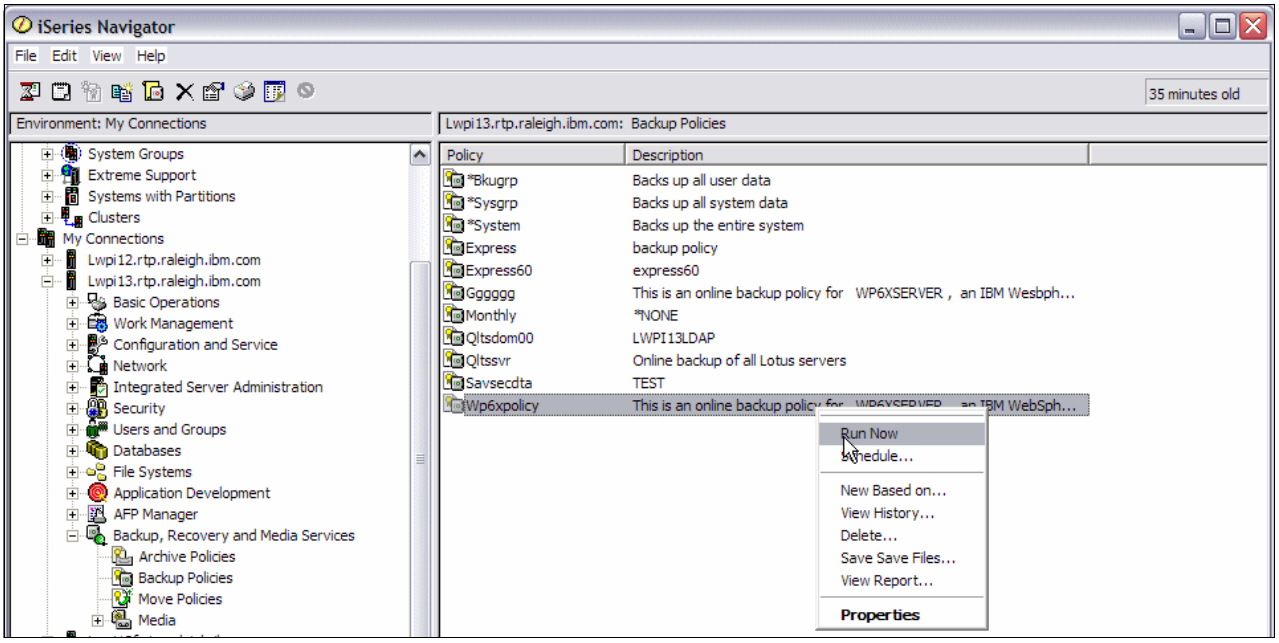


Figure 6-47 Running the backup policy

2. From the Backup Overrides window, do *not* select any options and click **OK** (Figure 6-48).

> **Note:** The example shows a customized setting. However, at any time you can override the setting and select a full backup. This is helpful if you want a full backup outside of the normal schedule.

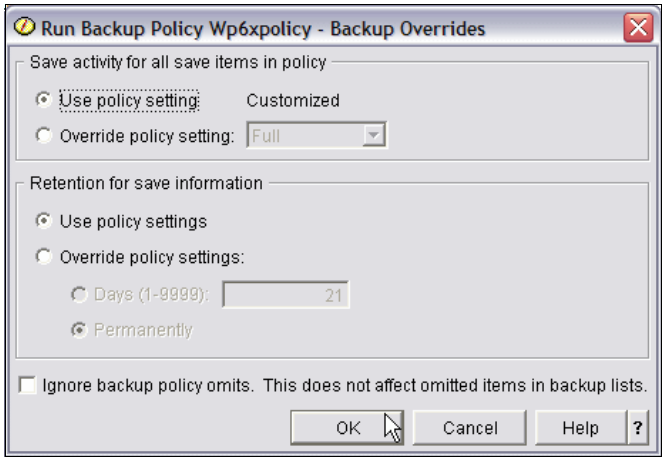

Run Backup Policy Wp6xpolicy - Backup Overrides
Save activity for all save items in policy
Use policy setting: Customized
Override policy setting: Full
Retention for save information
Use policy settings
Override policy settings:
Days (1-9999): 21
Permanently
Ignore backup policy omits. This does not affect omitted items in backup lists.
OK
Cancel
Help

Figure 6-48 Backup overrides

3. Depending on the settings for your user preferences within the iSeries Navigator client, you are shown messages about attempts to connect to the Management Central system. At this point, a connection is made to the Management Central system. You might get

messages that indicate the connection has been made. Click **OK** on the connection required panel if it is displayed.

> **Tip:** If you are getting errors connecting to the Management Central system, make sure your personal firewall is off. Network firewall issues might also cause the connection to fail.

4. Click **OK** on the Save Output (joblog) for BRMS Task window, if it is displayed.
5. The Backup operation is started as a task in Management Central. The window shown in Figure 6-49 is presented to confirm that the task has started and identifies the name of the task. This window then shows you the current status of the restore task and indicates whether the restore completed or failed.

> **Note:** Here is the corresponding i5/OS command line entry that invoked the back up:
>
> ```
> STRBKUBRM CTLGRP(wp6xpolicy) SCDTIME(*IMMED) SBMJOB(*YES) STRSEQ(*FIRST
> *FIRST) APPEND(*CTLGRPATR) ACTIVITY(*CTLGRPATR)
> ```

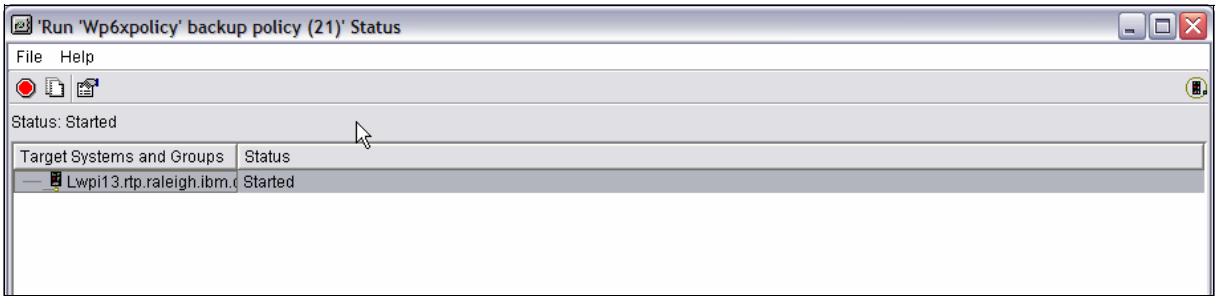


Figure 6-49 Backup task activity started

6. You can view the output of the task by selecting **Task Output** from the File menu.
7. A job log is shown. You can click any entry to get more information about the particular message (Figure 6-50). Notice also that the window title includes the job information. You can also view the job log from a 5250 emulation session. If there are any errors, correct them and rerun the backup policy.

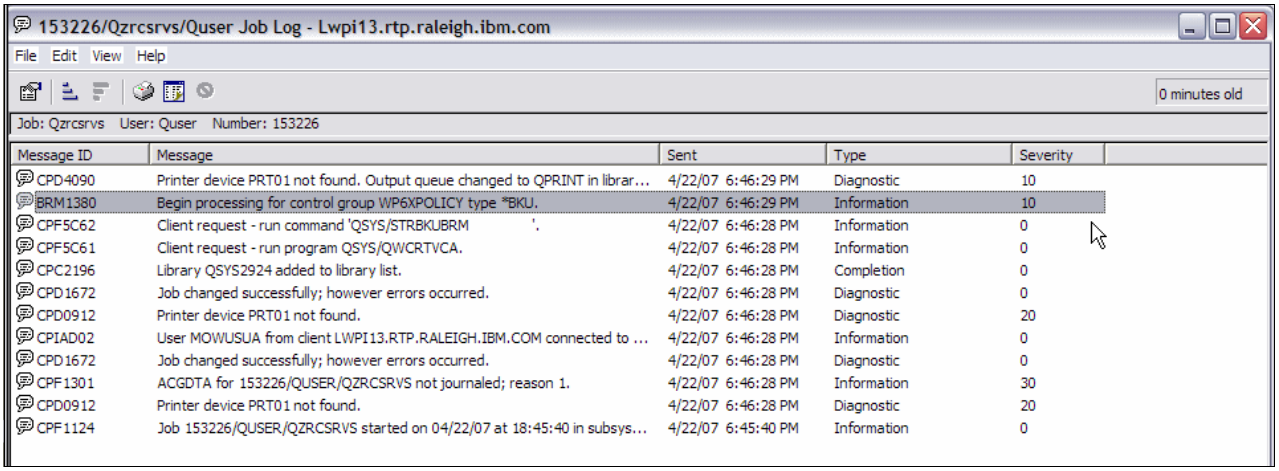

153226/Qzrcsrvs/Quser Job Log - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
0 minutes old
Job: Qzrcsrvs User: Quser Number: 153226
Message ID | Message | Sent | Type | Severity
CPD4090 | Printer device PRT01 not found. Output queue changed to QPRINT in librar... | 4/22/07 6:46:29 PM | Diagnostic | 10
BRM1380 | Begin processing for control group WP6XPOLICY type *BKU. | 4/22/07 6:46:29 PM | Information | 10
CPF5C62 | Client request - run command 'QSYS/STRBKUBRM '. | 4/22/07 6:46:28 PM | Information | 0
CPF5C61 | Client request - run program QSYS/QWCRTVCA. | 4/22/07 6:46:28 PM | Information | 0
CPC2196 | Library QSYS2924 added to library list. | 4/22/07 6:46:28 PM | Completion | 0
CPD1672 | Job changed successfully; however errors occurred. | 4/22/07 6:46:28 PM | Diagnostic | 0
CPD0912 | Printer device PRT01 not found. | 4/22/07 6:46:28 PM | Diagnostic | 20
CPIAD02 | User MOWUSUA from client LWPI13.RTP.RALEIGH.IBM.COM connected to ... | 4/22/07 6:46:28 PM | Information | 0
CPD1672 | Job changed successfully; however errors occurred. | 4/22/07 6:46:28 PM | Diagnostic | 0
CPF1301 | ACGDTA for 153226/QUSER/QZRCSRVS not journaled; reason 1. | 4/22/07 6:46:28 PM | Information | 30
CPD0912 | Printer device PRT01 not found. | 4/22/07 6:46:28 PM | Diagnostic | 20
CPF1124 | Job 153226/QUSER/QZRCSRVS started on 04/22/07 at 18:45:40 in subsys... | 4/22/07 6:45:40 PM | Information | 0

Figure 6-50 Job log entries

8. Upon completion, “Completed” is shown in the Status column (Figure 6-51).

Figure 6-51 Task completed successfully

9. You might also want to review the job log after completion to determine any warnings or informational messages that you need to correct.

6.4 Scenario 1: Restoring in one step from data saved with a backup policy

Important: You *must* load and apply PTF SI27222 for 5722BR1 before attempting to restore with the BRMS client.

This section describes how to restore saved data by using an online backup policy. You restore all saved objects (libraries and integrated file system files) in one step after completely removing all libraries and integrated file system files associated with the WebSphere Portal Express V6 profile.

In this example, you restore from a full backup. Following is a list of the activities performed in this section:

- Run the PreExpressRestore.sh script. This script ends the portal profile, if it is active, and cleans up the environment before restoring. It also makes a copy of the current profile registry located in /QIBM/UserData/WebSphere/AppServer/V6/Base/profileRegistry/profileregistry.xml. The new copy is called profileregistryOrig.xml. You must run this script if you want to use the BRMS restore wizard to select all saved components (libraries and stream files) for restore in one step.
- Run the BRMS restore wizard to restore all the data saved with the backup policy.
- Run the PostBRMSRestore.sh script after the restore. This script restores the user profiles that correspond to the portal profile’s Database Administrator. It also restores or grants the necessary authorities for that profile. Lastly, the script restores the private authorities of QTMHHTTP and QEJBSVR for the objects restored.

Note: For 5250 emulation session users, use the following command to perform the same steps in this section. Enter the command and press F4 to prompt it.

```
WRKMEDIBRM CTLGRP(WP6XPOLICY) SLTDATE(*BEGIN *END)
```

WP6XPOLICY is the name of the backup policy. Use option 7 to restore all items.

6.4.1 Running the PreExpressRestore.sh script

Perform the following steps to run the PreExpressRestore.sh script:

1. From the iSeries Navigator, right-click the connection entry for your i5/OS system and select **Run Command** (Figure 6-52).

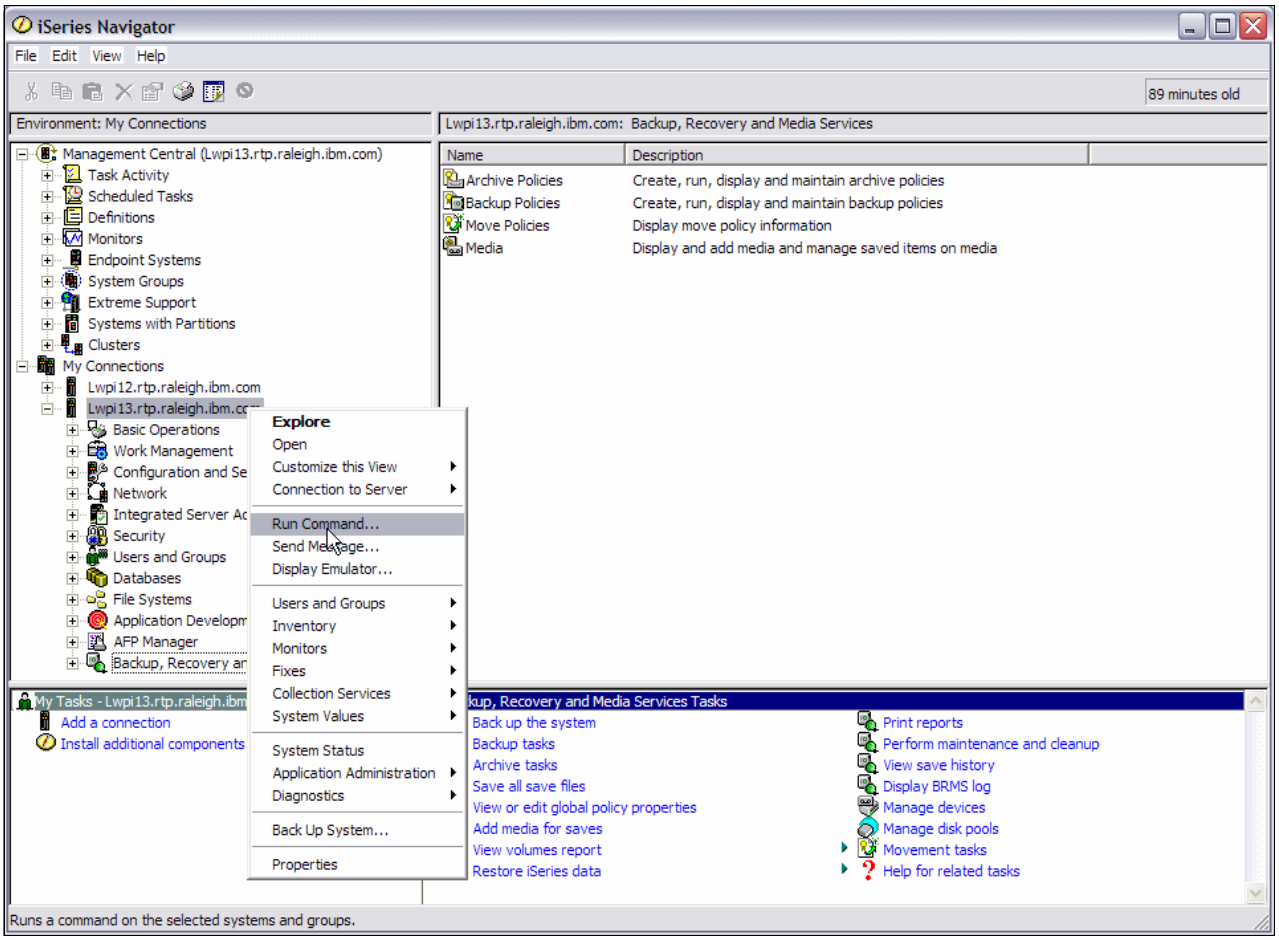


Figure 6-52 Selecting to run i5/OS commands from iSeries Navigator

2. On the General tab of the Run Command window (Figure 6-53), enter the following command to run the PreExpressRestore.sh script:

   ```
   STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/PreExpressRestore.sh -p
   <profilename>')
   ```

   For our example, this is:

   ```
   STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/PreExpressRestore.sh -p
   wp6xserver')
   ```

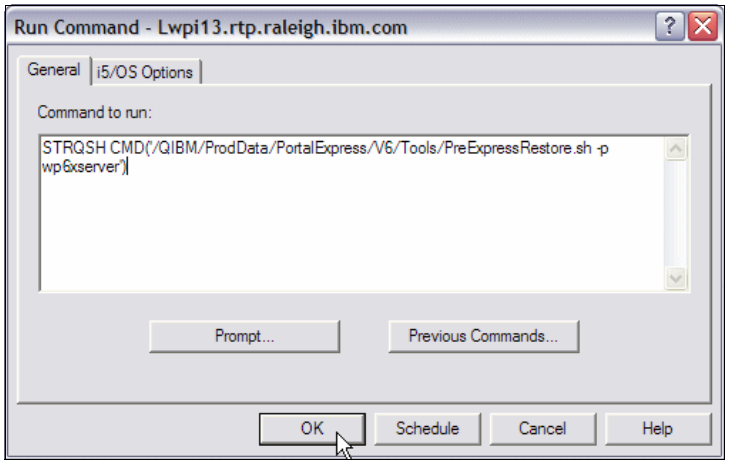


Figure 6-53 Running the PreExpressRestore.sh script

3. A connection is made to the Management Central system. You might be notified that the activity has started. Click **OK** if it is displayed.
4. The **Run Command Status** window shows the status of the command. It shows a status of Completed when it is done as shown in Figure 6-54. If the command fails, make sure you have entered the command correctly and rerun the command. You can explore the status panel to obtain more information about the task output.

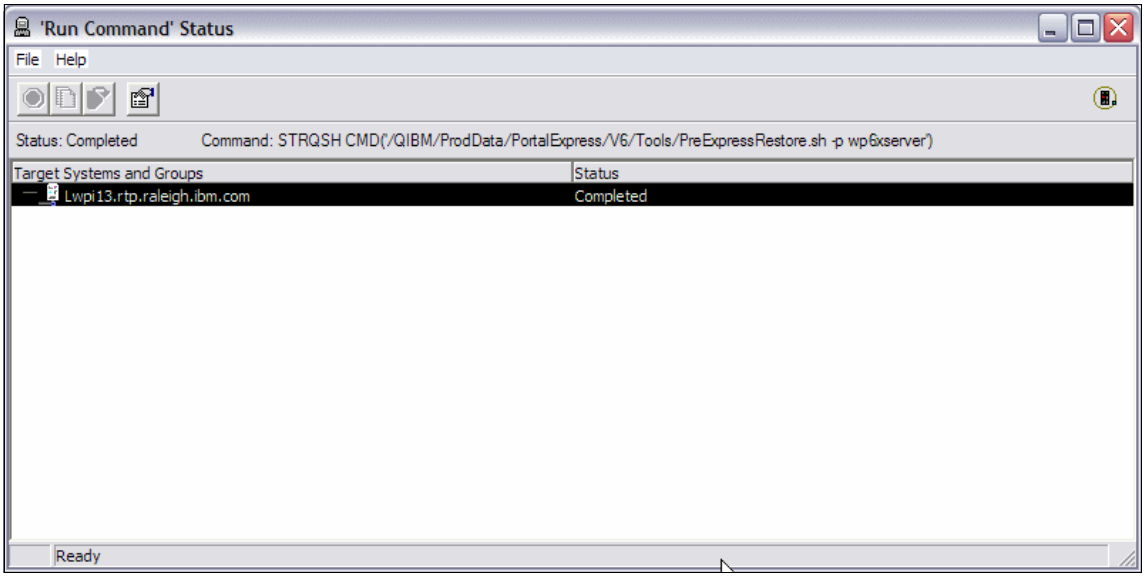


Figure 6-54 PreExpressRestore.sh script ran successfully

5. Alternatively, you can run the PreExpressRestore.sh script from the i5/OS QShell environment. Log in to the i5/OS QShell environment (STRQSH) and run the following command:

   ```
   /QIBM/ProdData/PortalExpress/V6/Tools/PreExpressRestore.sh -p <profilename>
   ```

   For our example, this is:

   ```
   /QIBM/ProdData/PortalExpress/V6/Tools/PreExpressRestore.sh -p wp6xserver
   ```

6.4.2 Restoring all saved components in one step

Perform the following commands to restore all the saved components in one step:

1. From the iSeries Navigator, right-click **Backup, Recovery and Media Services** and select **Restore** (Figure 6-55).

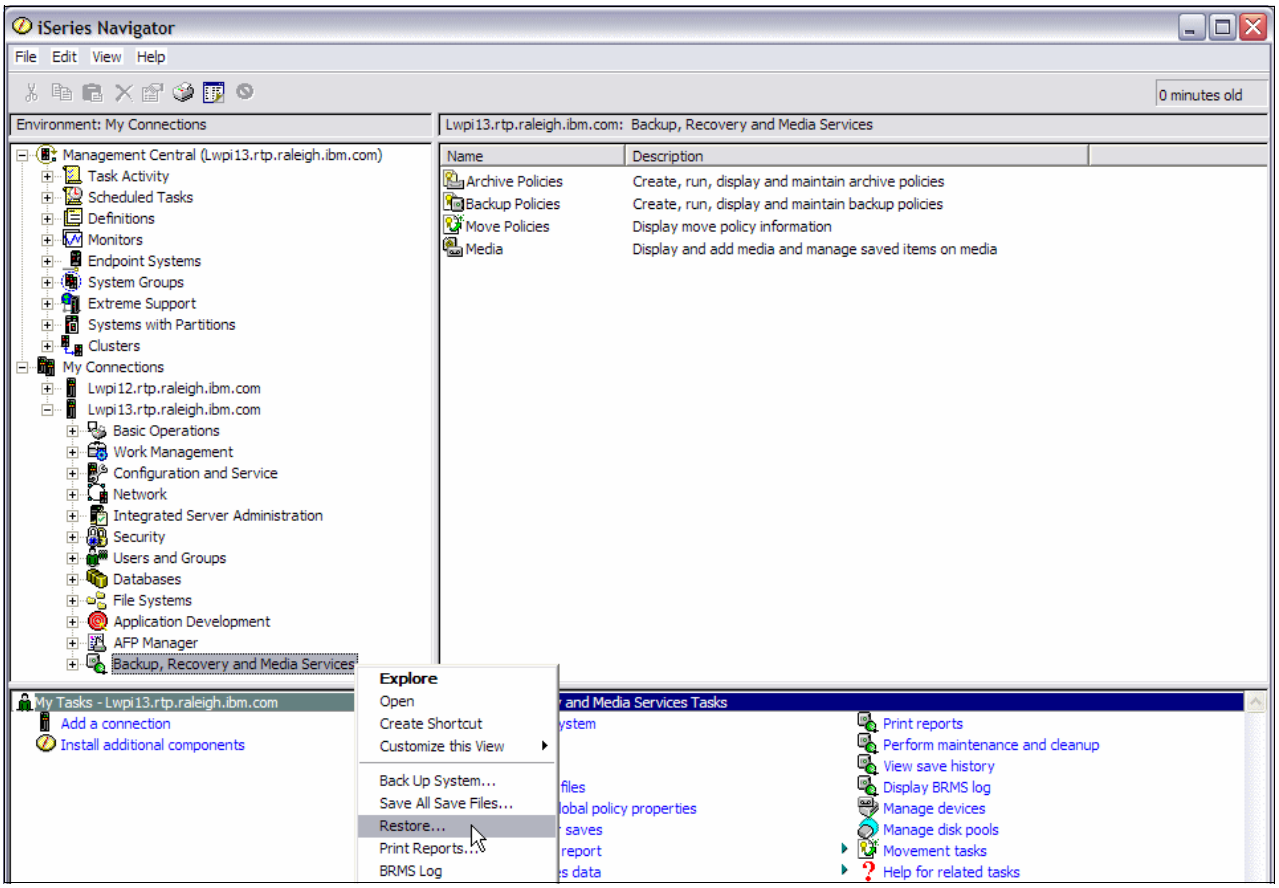


Figure 6-55 Use the restore option of BRMS

2. An informational message is displayed (Figure 6-56). Click **OK** to continue.

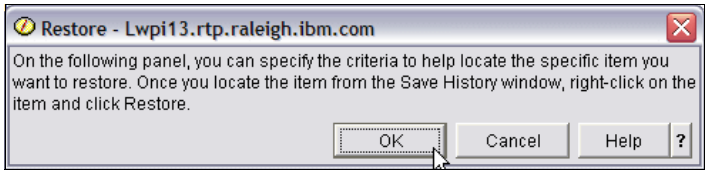

Restore - Lwpi13.rtp.raleigh.ibm.com
On the following panel, you can specify the criteria to help locate the specific item you want to restore. Once you locate the item from the Save History window, right-click on the item and click Restore.
OK
Cancel
Help
?

Figure 6-56 Restore informational message

3. On the Save History - Include window (Figure 6-57), you can define the criteria for your restore:
   - Policy: The policy used for the backup, if any. For our example, we enter `wp6xpolicy`.
   - Save dates: Dates of the backup from which you want to restore from. Select **Specify dates**.
   - From - To: Exact dates of the backup you want to use.
   - Completion Status: Select **Successful saves**.
   - System: This is where the objects were saved. Select **Local System**.

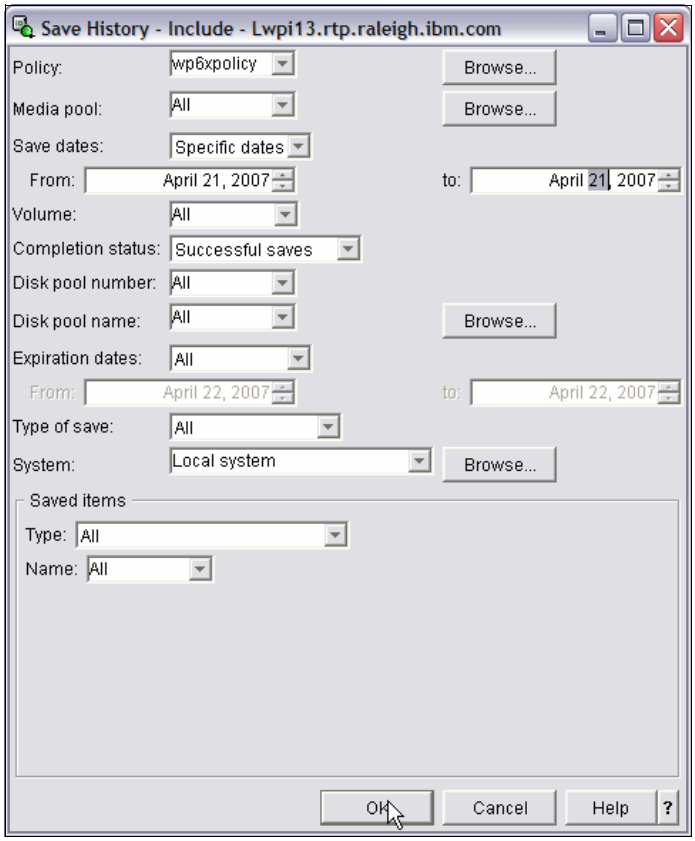


Figure 6-57 Specifying the restore criteria

4. The next window shows the various folder, object, and directory lists that match the criteria you selected in the last step. In this window, you can select individual entries or all the data for a backup. Hold the shift key and select all the folders, libraries, and objects that you want. In our example, we want to restore everything that was backed up from the full backup and the latest cumulative changes save. Right-click the selection you have made and select **Restore.** See the *BRMS iSeries Navigator Client Student Guide* for additional information (Figure 6-58).

> **Important:** We are not restoring any of the QUSRBRM library's content. This library contains media information and is normally used for major disaster recovery situations. Consult the BRMS guide for more information.

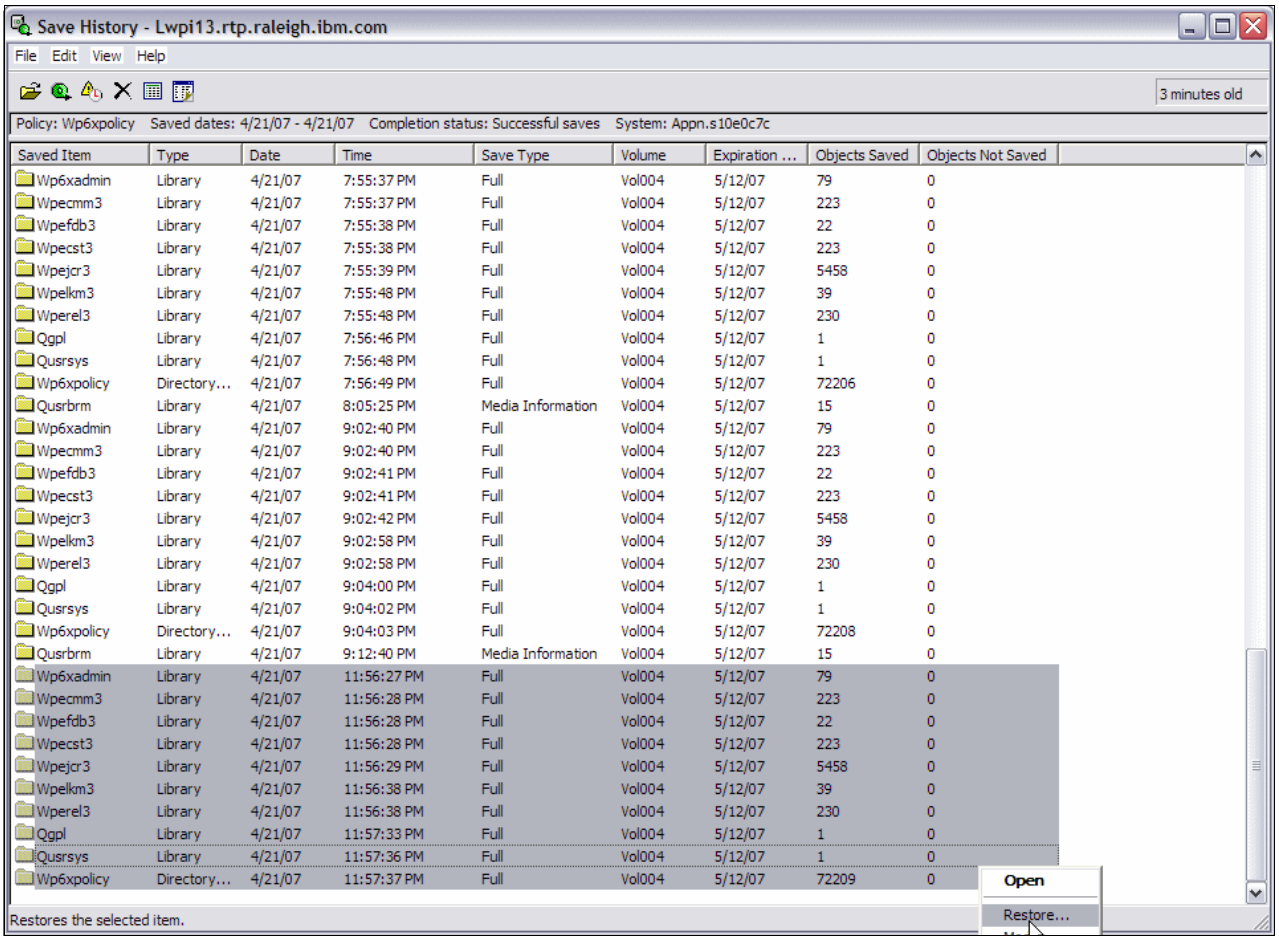

Save History - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
3 minutes old
Policy: Wp6xpolicy Saved dates: 4/21/07 - 4/21/07 Completion status: Successful saves System: Appn.s10e0c7c
Saved Item | Type | Date | Time | Save Type | Volume | Expiration ... | Objects Saved | Objects Not Saved
Wp6xadmin Library 4/21/07 7:55:37 PM Full Vol004 5/12/07 79 0
Wpecmm3 Library 4/21/07 7:55:37 PM Full Vol004 5/12/07 223 0
Wpefdb3 Library 4/21/07 7:55:38 PM Full Vol004 5/12/07 22 0
Wpecst3 Library 4/21/07 7:55:38 PM Full Vol004 5/12/07 223 0
Wpejcr3 Library 4/21/07 7:55:39 PM Full Vol004 5/12/07 5458 0
Wpelkm3 Library 4/21/07 7:55:48 PM Full Vol004 5/12/07 39 0
Wperel3 Library 4/21/07 7:55:48 PM Full Vol004 5/12/07 230 0
Qgpl Library 4/21/07 7:56:46 PM Full Vol004 5/12/07 1 0
Qusrsys Library 4/21/07 7:56:48 PM Full Vol004 5/12/07 1 0
Wp6xpolicy Directory... 4/21/07 7:56:49 PM Full Vol004 5/12/07 72206 0
Qusrbrm Library 4/21/07 8:05:25 PM Media Information Vol004 5/12/07 15 0
Wp6xadmin Library 4/21/07 9:02:40 PM Full Vol004 5/12/07 79 0
Wpecmm3 Library 4/21/07 9:02:40 PM Full Vol004 5/12/07 223 0
Wpefdb3 Library 4/21/07 9:02:41 PM Full Vol004 5/12/07 22 0
Wpecst3 Library 4/21/07 9:02:41 PM Full Vol004 5/12/07 223 0
Wpejcr3 Library 4/21/07 9:02:42 PM Full Vol004 5/12/07 5458 0
Wpelkm3 Library 4/21/07 9:02:58 PM Full Vol004 5/12/07 39 0
Wperel3 Library 4/21/07 9:02:58 PM Full Vol004 5/12/07 230 0
Qgpl Library 4/21/07 9:04:00 PM Full Vol004 5/12/07 1 0
Qusrsys Library 4/21/07 9:04:02 PM Full Vol004 5/12/07 1 0
Wp6xpolicy Directory... 4/21/07 9:04:03 PM Full Vol004 5/12/07 72208 0
Qusrbrm Library 4/21/07 9:12:40 PM Media Information Vol004 5/12/07 15 0
Wp6xadmin Library 4/21/07 11:56:27 PM Full Vol004 5/12/07 79 0
Wpecmm3 Library 4/21/07 11:56:28 PM Full Vol004 5/12/07 223 0
Wpefdb3 Library 4/21/07 11:56:28 PM Full Vol004 5/12/07 22 0
Wpecst3 Library 4/21/07 11:56:28 PM Full Vol004 5/12/07 223 0
Wpejcr3 Library 4/21/07 11:56:29 PM Full Vol004 5/12/07 5458 0
Wpelkm3 Library 4/21/07 11:56:38 PM Full Vol004 5/12/07 39 0
Wperel3 Library 4/21/07 11:56:38 PM Full Vol004 5/12/07 230 0
Qgpl Library 4/21/07 11:57:33 PM Full Vol004 5/12/07 1 0
Qusrsys Library 4/21/07 11:57:36 PM Full Vol004 5/12/07 1 0
Wp6xpolicy Directory... 4/21/07 11:57:37 PM Full Vol004 5/12/07 72209 0
Open
Restore...
Restores the selected item.

Figure 6-58 Selecting data for a restore

5. On the Restore wizard Welcome window (Figure 6-59), click **Next**.

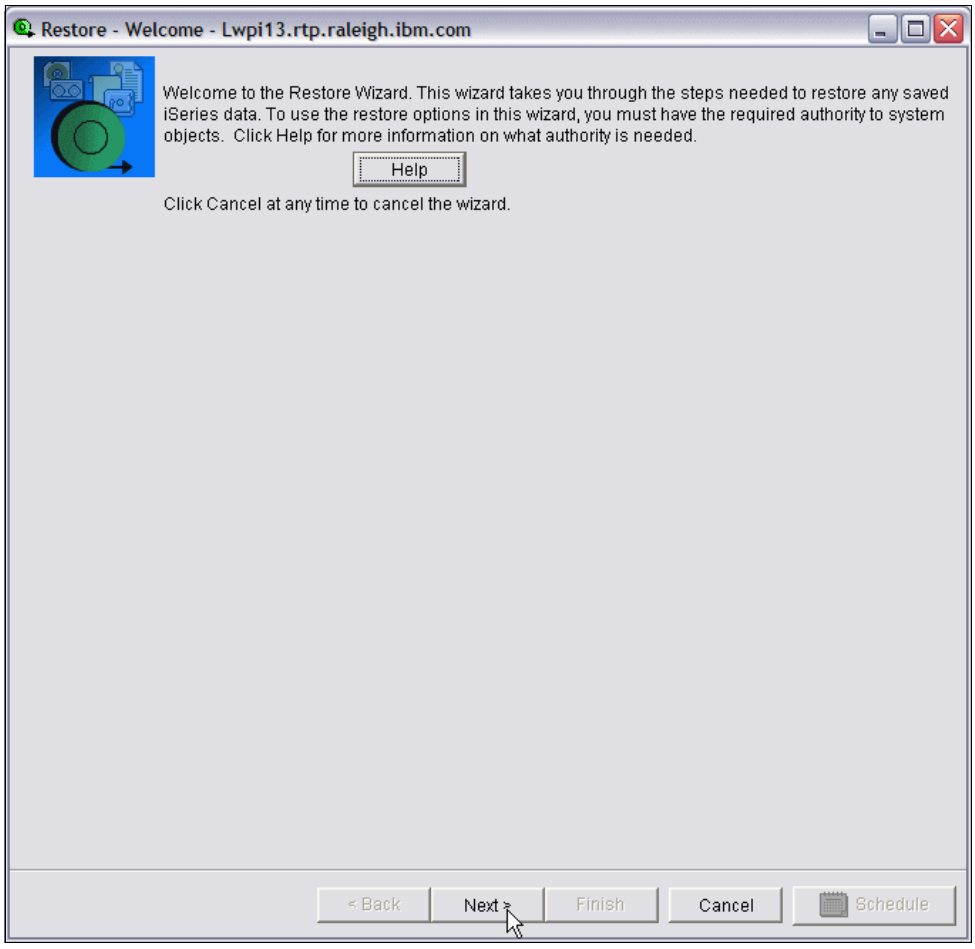

Restore - Welcome - Lwpi13.rtp.raleigh.ibm.com
Welcome to the Restore Wizard. This wizard takes you through the steps needed to restore any saved iSeries data. To use the restore options in this wizard, you must have the required authority to system objects. Click Help for more information on what authority is needed.
Help
Click Cancel at any time to cancel the wizard.
< Back
Next >
Finish
Cancel
Schedule

Figure 6-59 Restore wizard Welcome window

6. You are shown objects that you chose to restore. Next, the journal objects information window is shown. The choice of the whether or not to apply the changes and the dates of the changes varies, depending on the reason for the restore. For many cases, you might want to restore a particular point in time because that was when you were sure the data was good. In our example, we want to restore all changes that are available.

   For our example, we use the default of the selected check box for **Restore journal receivers** and selected radio button of **Apply journal changes to the current data and time**. Click **Next** (Figure 6-60).

   Note: Depending on the recovery objectives, you need to consider saving all changed journal receivers periodically. During a disaster recovery event, if all required journal receivers were saved periodically, then BRMS can perform recovery up to the last commitment boundary based on the last saved journal receivers. Journal receivers contain database update information that can replay to perform point in time recovery. For more information, see the IBM Redpaper *Improve Whole System Backups with the New Save-While-Active Function*, REDP-7200, at:

   http://www.redbooks.ibm.com/abstracts/redp7200.html

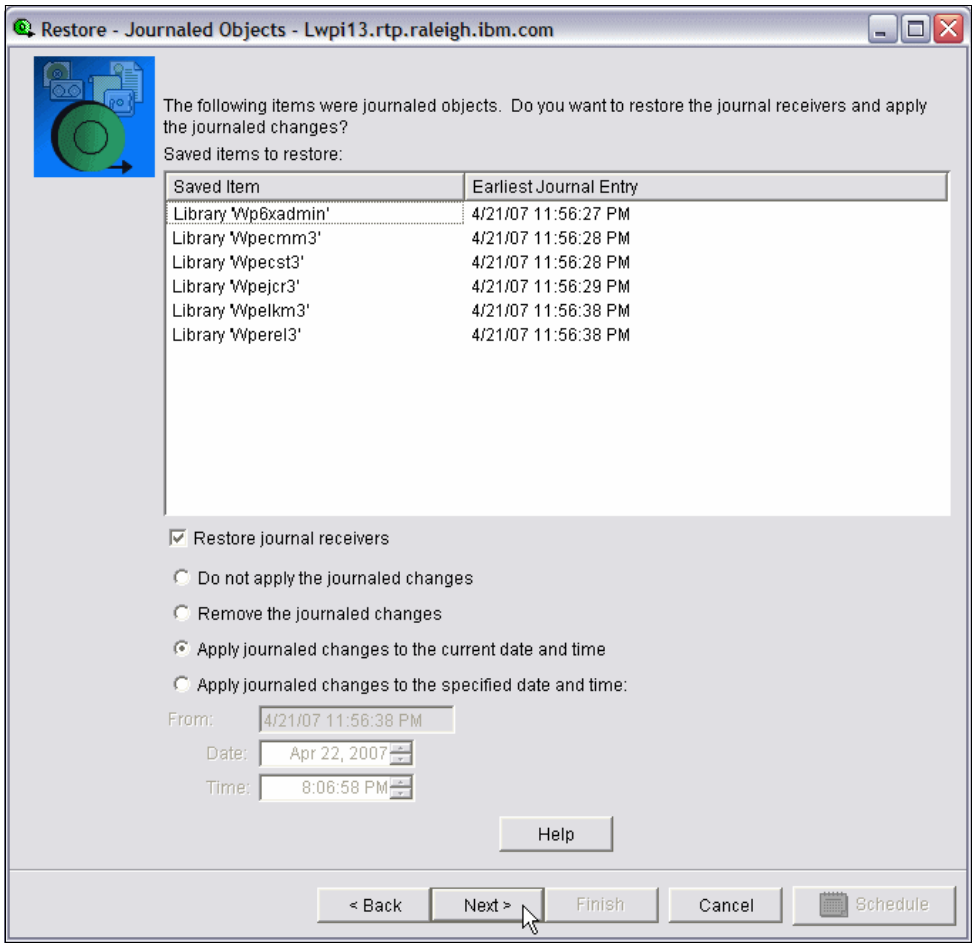

Restore - Journaled Objects - Lwpi13.rtp.raleigh.ibm.com
The following items were journaled objects. Do you want to restore the journal receivers and apply the journaled changes?
Saved items to restore:
Saved Item
Earliest Journal Entry
Library 'Wp6xadmin' 4/21/07 11:56:27 PM
Library 'Wpecmm3' 4/21/07 11:56:28 PM
Library 'Wpecst3' 4/21/07 11:56:28 PM
Library 'Wpejcr3' 4/21/07 11:56:29 PM
Library 'Wpelkm3' 4/21/07 11:56:38 PM
Library 'Wperel3' 4/21/07 11:56:38 PM
Restore journal receivers
Do not apply the journaled changes
Remove the journaled changes
Apply journaled changes to the current date and time
Apply journaled changes to the specified date and time:
From: 4/21/07 11:56:38 PM
Date: Apr 22, 2007
Time: 8:06:58 PM
Help
< Back
Next >
Finish
Cancel
Schedule

Figure 6-60 Journal changes selection

7. On the Restore Directory window (Figure 6-61), select **Restore directory and all files** and select the **Include subdirectories** check box. Click **Next**.

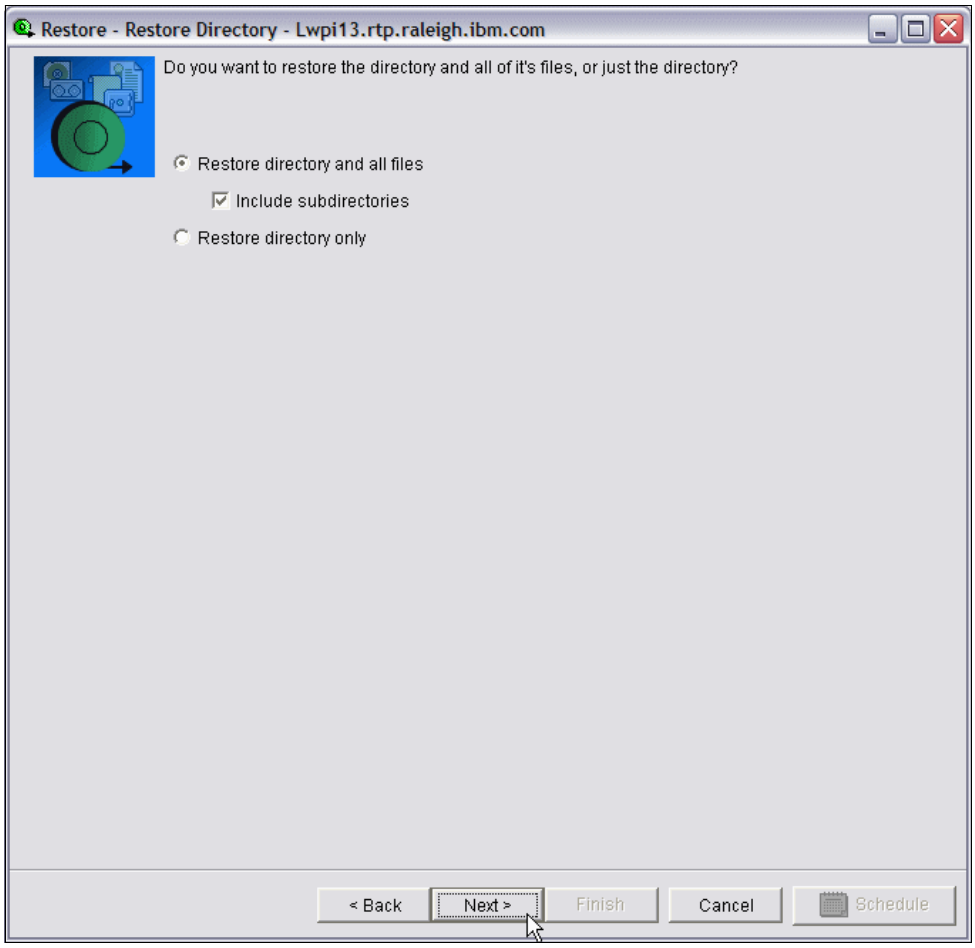

Restore - Restore Directory - Lwpi13.rtp.raleigh.ibm.com
Do you want to restore the directory and all of it's files, or just the directory?
Restore directory and all files
Include subdirectories
Restore directory only
< Back
Next >
Finish
Cancel
Schedule

Figure 6-61 Specifying restore directory and files information

8. On the Use Save History Device window (Figure 6-62), you have the option of selecting the device to restore. You can select the particular devices if known. Otherwise, let it select automatically. Click **Next**.

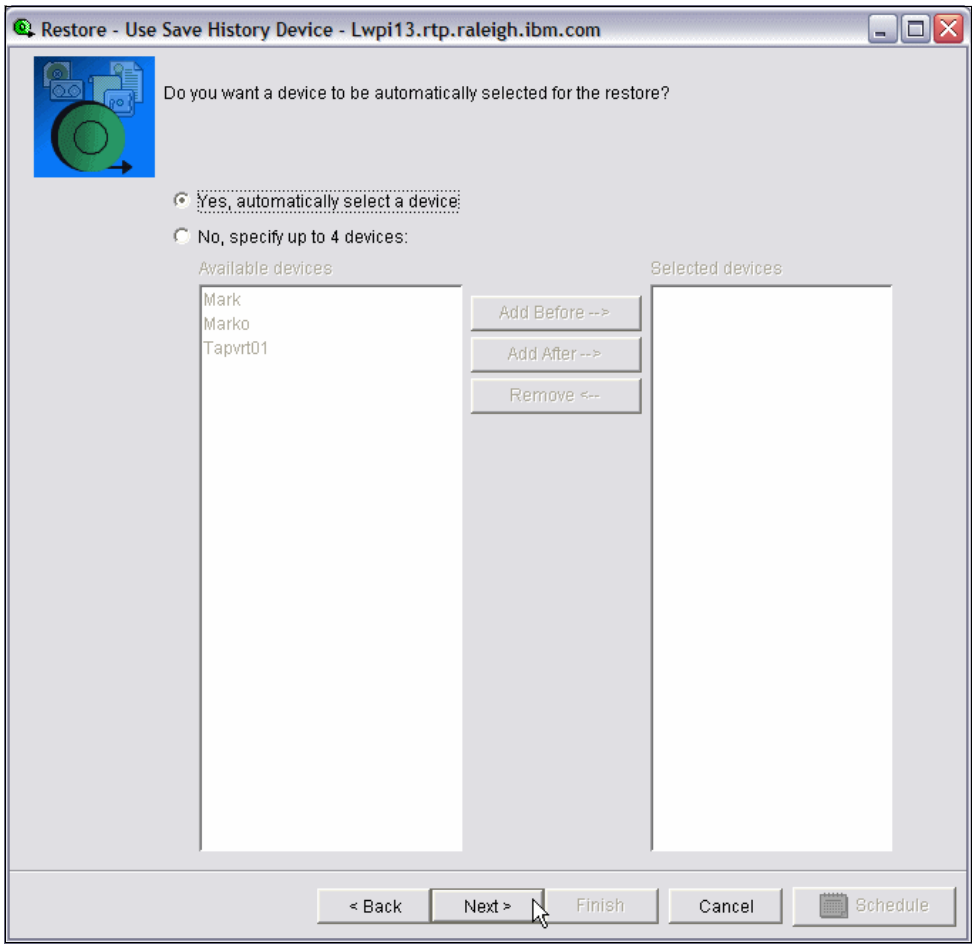


Figure 6-62 Automatically selecting a device for the restore

9. On the Summary window (Figure 6-63), you can inspect what you intend to restore. You can click **Details** to see a list of the files to restore. Click **Advanced Options**.

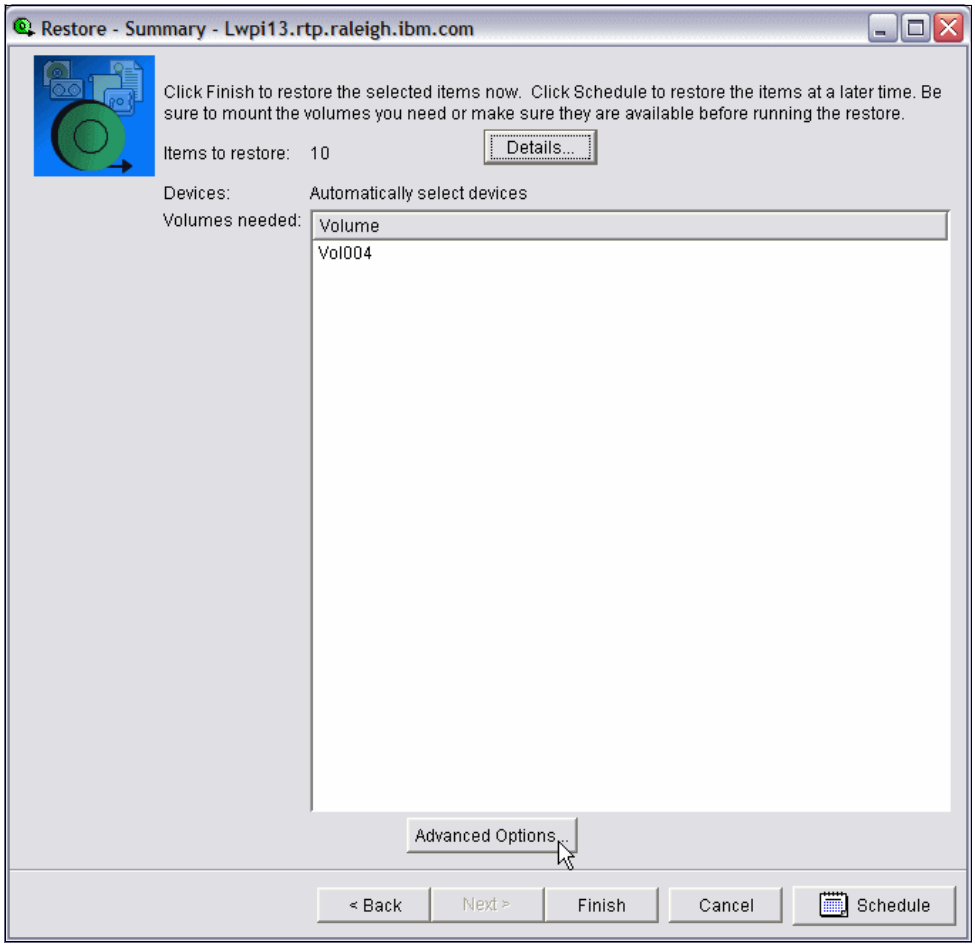

Restore - Summary - Lwpi13.rtp.raleigh.ibm.com
Click Finish to restore the selected items now. Click Schedule to restore the items at a later time. Be sure to mount the volumes you need or make sure they are available before running the restore.
Items to restore: 10
Details...
Devices: Automatically select devices
Volumes needed:
Volume
Vol004
Advanced Options...
< Back
Next >
Finish
Cancel
Schedule

Figure 6-63 Summary of the restore

10. On the Restore - Advanced Options window (Figure 6-64), click **OK** when done.

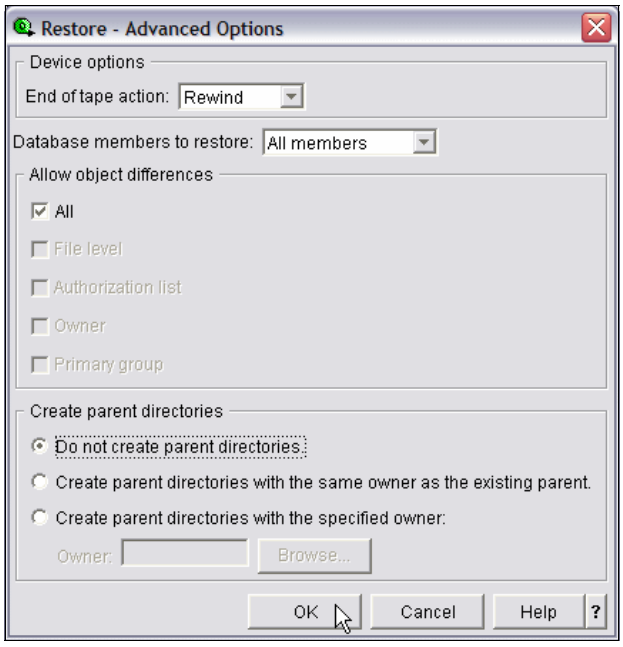


Figure 6-64 Selecting the advanced restore options

11. Back on the Restore - Summary window, click **Finish** to start the restore (Figure 6-65).

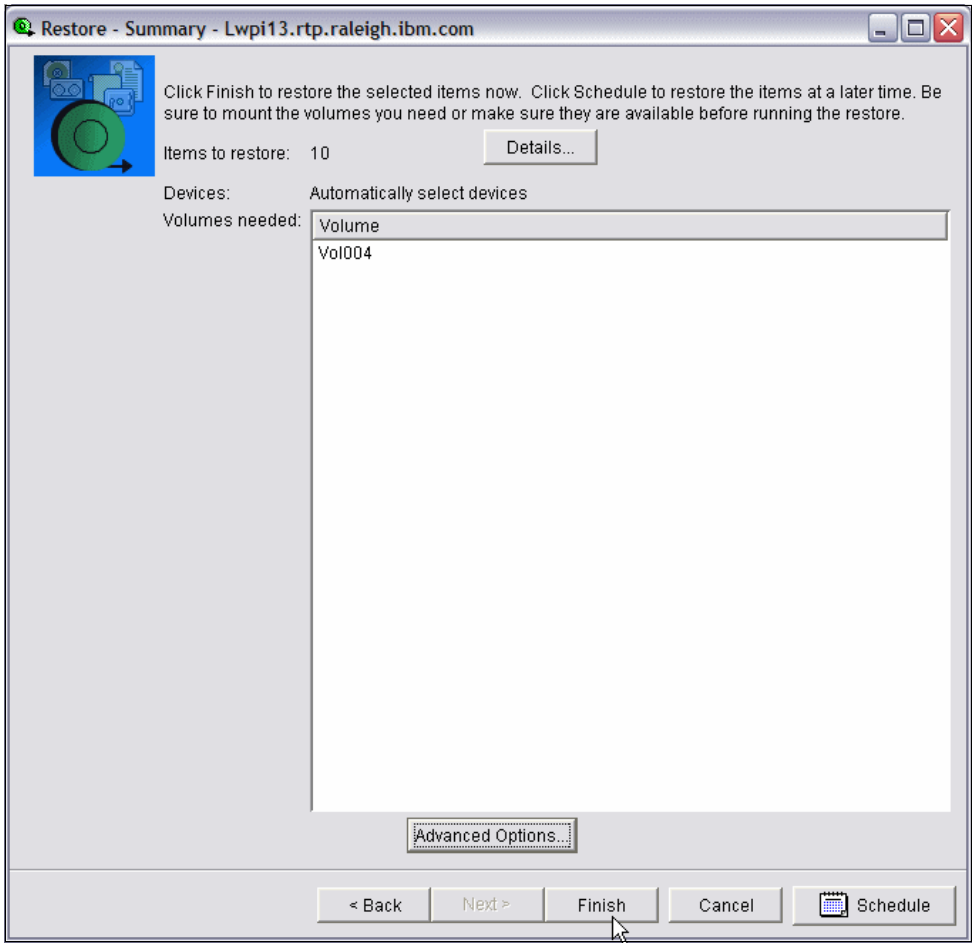

Restore - Summary - Lwpi13.rtp.raleigh.ibm.com
Click Finish to restore the selected items now. Click Schedule to restore the items at a later time. Be sure to mount the volumes you need or make sure they are available before running the restore.
Items to restore: 10
Details...
Devices: Automatically select devices
Volumes needed:
Volume
Vol004
Advanced Options...
< Back
Next >
Finish
Cancel
Schedule

Figure 6-65 Starting the restore

12. At this point, a connection is made to the Management Central system. You might get messages that indicate the connection has been made. Click **OK** on the connection required panel if it is displayed.
13. Click **OK** on the Save Output (joblog) for BRMS Task window, if it is displayed.
14. The restore operation is started as a task in Management Central. The window shown in Figure 6-66 is presented to confirm that the task has started. It identifies the name of the task and where you can view the status. Click **OK**.

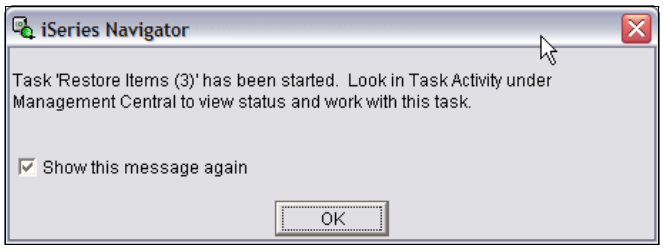

iSeries Navigator
Task 'Restore Items (3)' has been started. Look in Task Activity under Management Central to view status and work with this task.
Show this message again
OK

Figure 6-66 Restore task activity

15. The Restore Items Status window (Figure 6-67) is presented to show you the current status of the restore request. It indicates whether the restore completed or failed.

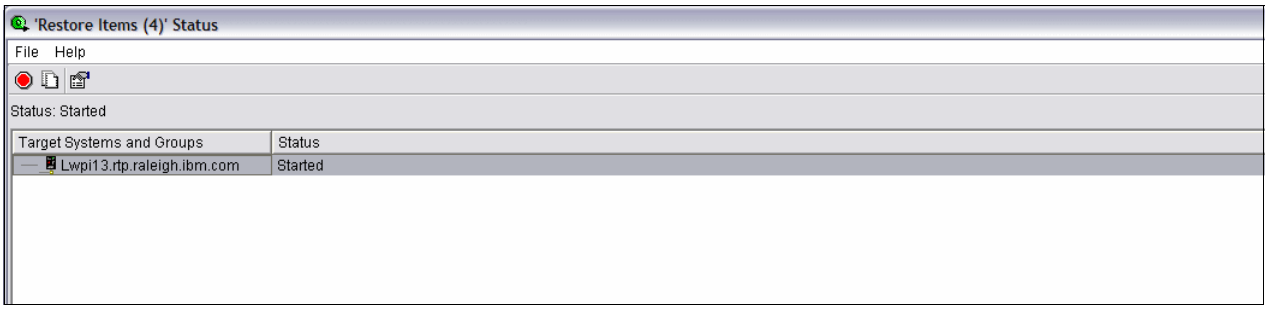


Figure 6-67 Restore status

16. You can view the output of the task by selecting **Task Output** from the File menu. (Figure 6-68).

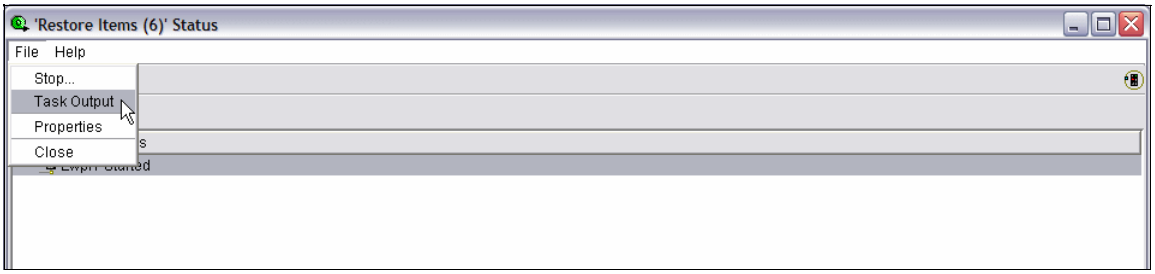


Figure 6-68 Accessing the joblog for the restore

6.4.3 Running the PostExpressRestore.sh script

Perform the following steps to run the PostExpressRestore.sh script:

1. From the iSeries Navigator, right-click the connection entry for your i5/OS system and select **Run Command** (Figure 6-69).

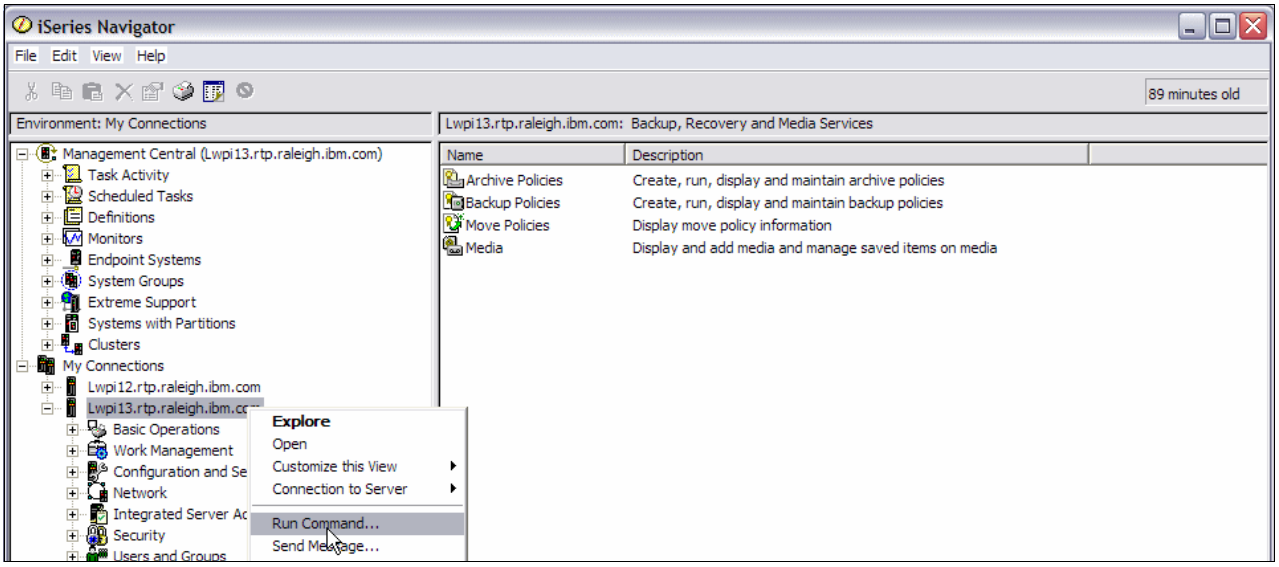


Figure 6-69 Selecting to run i5/OS commands from iSeries Navigator

2. On the General tab of the Run Command window (Figure 6-53 on page 293), enter the following command to run the PostExpressRestore.sh script:

   ```
   STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/PostExpressRestore.sh -p
   <profilename>')
   ```

   For our example, this is:

   ```
   STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/PostExpressRestore.sh -p
   wp6xserver')
   ```

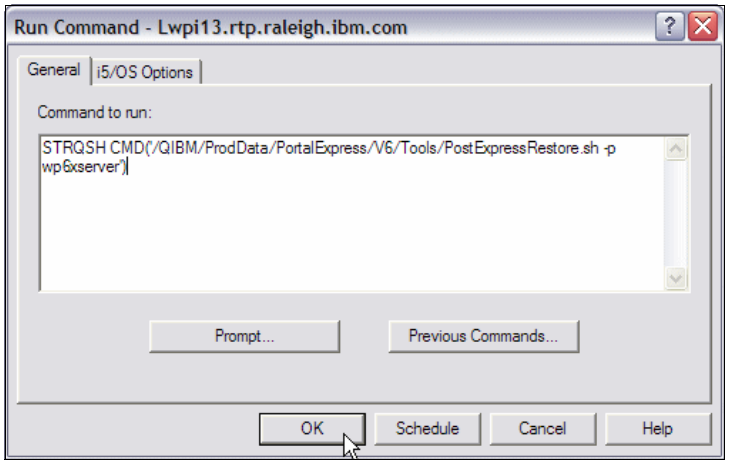


Figure 6-70 Running the PostExpressRestore.sh script

3. A connection is made to the Management Central system. You might be notified that the activity has started. Click **OK** if it is displayed.
4. The **Run Command Status** window shows the status of the command. It shows a status of Completed when it is done as shown in Figure 6-71. If the command fails, make sure you have entered the command correctly and rerun the command. You can explore the status panel to obtain more information about the task output.

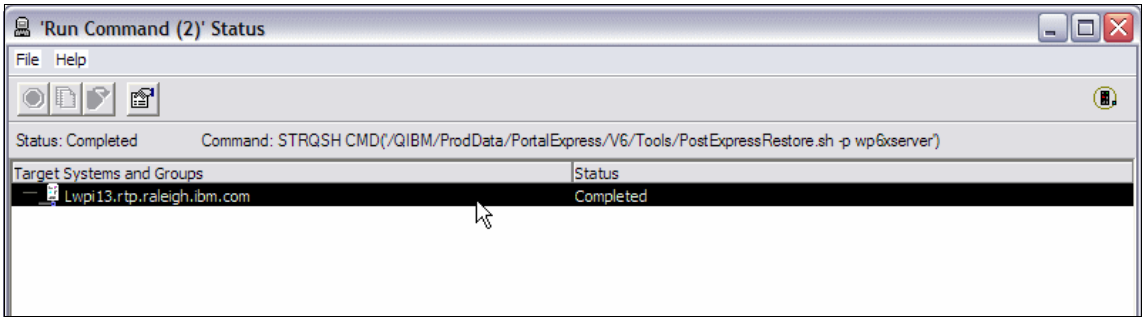


Figure 6-71 PostExpressRestore.sh script ran successfully

5. Alternatively, you can run the PostExpressRestore.sh script from the i5/OS QShell environment. Log in to the i5/OS QShell environment (STRQSH) and run the following command:

   ```
   /QIBM/ProdData/PortalExpress/V6/Tools/PostExpressRestore.sh -p <profilename>
   ```

   For our example, this is:

   ```
   /QIBM/ProdData/PortalExpress/V6/Tools/PostExpressRestore.sh -p wp6xserver
   ```

6. When the restore is completed, compare the newly restored profileregistry.xml and profileregistryOrig.xml files in the /QIBM/UserData/WebSphere/AppServer/V6/Base/profileRegistry folder. Assuming the content of the files is different, you might want to merge them so that the resulting profileregistry.xml contains an entry for every portal profile configured on the system. In most cases, you do not need to perform any action. Lastly, it is a good practice to clean out the profileregistryOrig.xml file.

6.5 Scenario 2: Restoring individually from data saved with a backup policy

In this restore scenario, we show an example where each of the schema or database libraries, integrated file system objects, database owner user profile and security data, and HTTP server member object are restored separately from each other. While this lengthens the time to restore, it also allows for more control over the restore process.

Following is a list of the activities described in this section:

- “Running the PreExpressRestore.sh script” on page 306
- “Restoring all schemas and database libraries” on page 306
- “Restoring the HTTP server member object” on page 317
- “Restoring user profile and security data” on page 319
- “Restoring the integrated file system files” on page 320
- “Running the PostExpressRestore.sh script” on page 327

6.5.1 Running the PreExpressRestore.sh script

For details about running the PreExpressRestore,sh script, see 6.4.1, “Running the PreExpressRestore.sh script” on page 292.

6.5.2 Restoring all schemas and database libraries

This section describes how to restore all the schemas or databases and their associated libraries. There are seven databases or schemas that you need to restore. One interesting thing is that we restore one database at a time. This is because after each schema is restored, the user can review the logs for any errors and make sure everything is restored.

Following is the list of schemas or databases to restore:

- RELEASE database
- CUSTOMIZATION database
- COMMUNITY database
- JCR database
- WMM database
- FEEDBACK database
- LIKEMINDS database

For our example, we restore the following databases:

- Release database: WPEREL3
- Customization database: WPECUS3
- Community database: WPECMM3
- JCR database: WPEJCR3
- WMM database: WP6XADMIN

- Feedback database: WPEFDB3
- Likeminds database: WPELKM3

Restoring the RELEASE database

Perform the following steps to restore the RELEASE database:

1. From the iSeries Navigator, right-click **Backup, Recovery and Media Services** and select **Restore** (Figure 6-72).

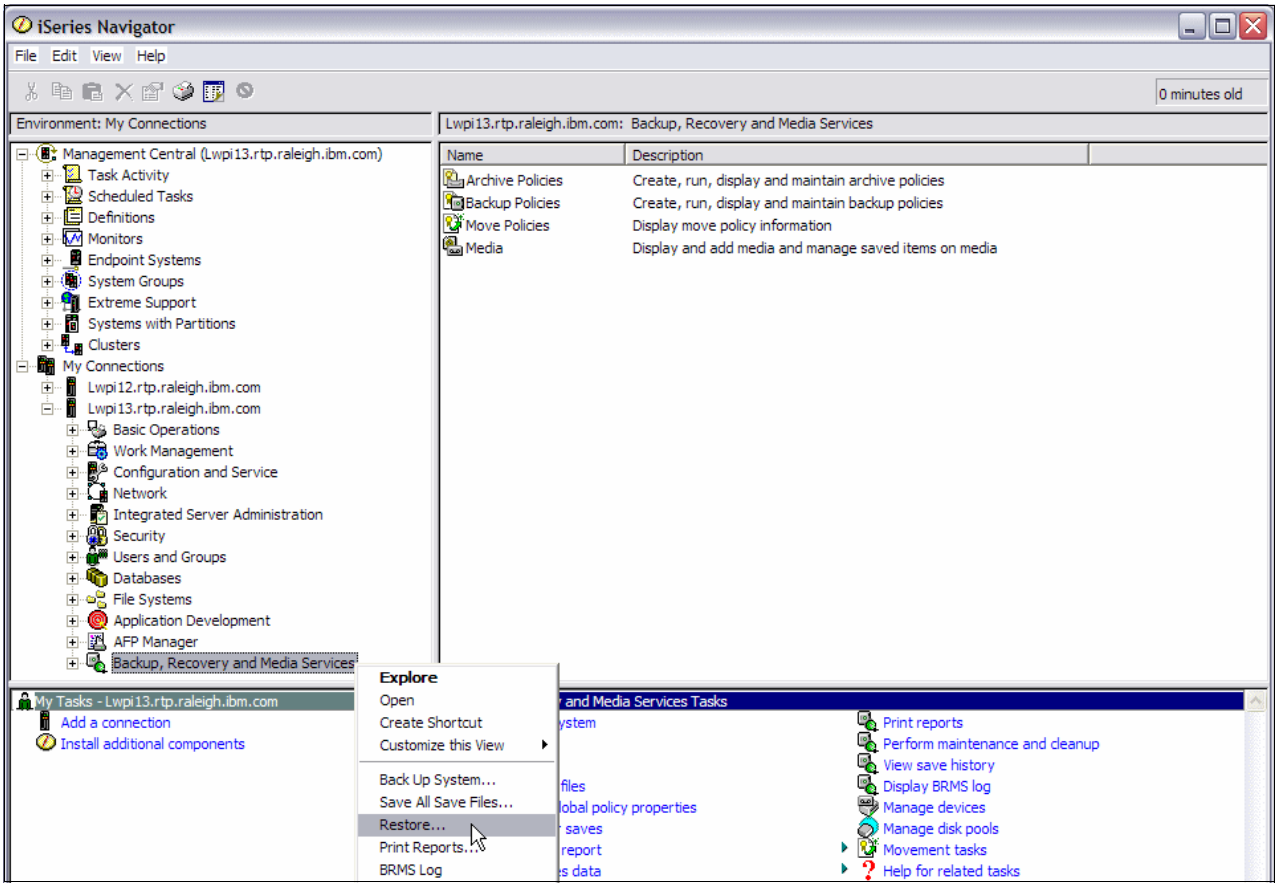


Figure 6-72 Selecting the BRMS restore option

2. An informational message is displayed (Figure 6-73). Click **OK** to continue.

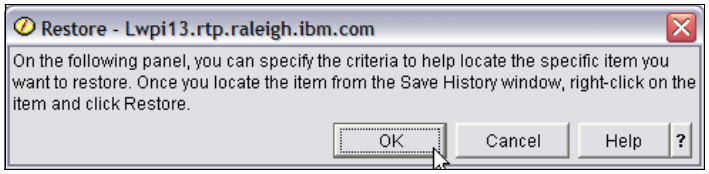

Restore - Lwpi13.rtp.raleigh.ibm.com
On the following panel, you can specify the criteria to help locate the specific item you want to restore. Once you locate the item from the Save History window, right-click on the item and click Restore.
OK
Cancel
Help

Figure 6-73 Restore informational message

3. On the Save History - Include window (Figure 6-74), you can define the criteria for your restore:
   - Policy: The policy used for the backup, if any. For our example, we enter `wp6xpolicy`.
   - Save dates: Dates of the backup from which you want to restore. Select **Specify dates**.
   - From - To: Exact dates of the backup you want to use.
   - Completion status: Select **Successful saves**.
   - System: This is where the objects were saved. Select **Local System**.

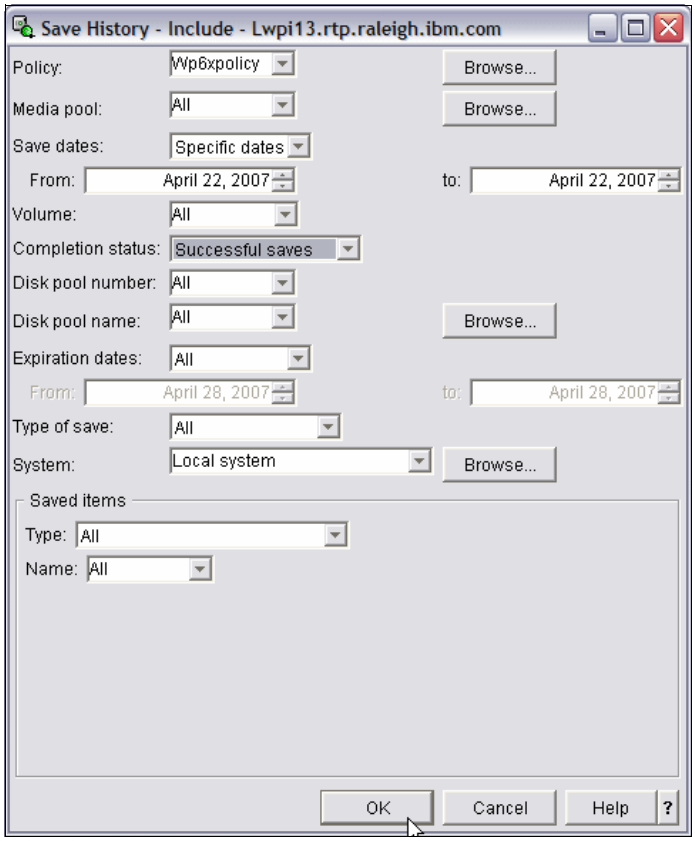


Figure 6-74 Specifying the restore criteria

4. The Save History window (Figure 6-75) shows the various folder, object, and directory lists that match the criteria you selected in the last step. Select the **Release** database. For our example, this is WPEREL3. Right-click the database and select **Restore**.

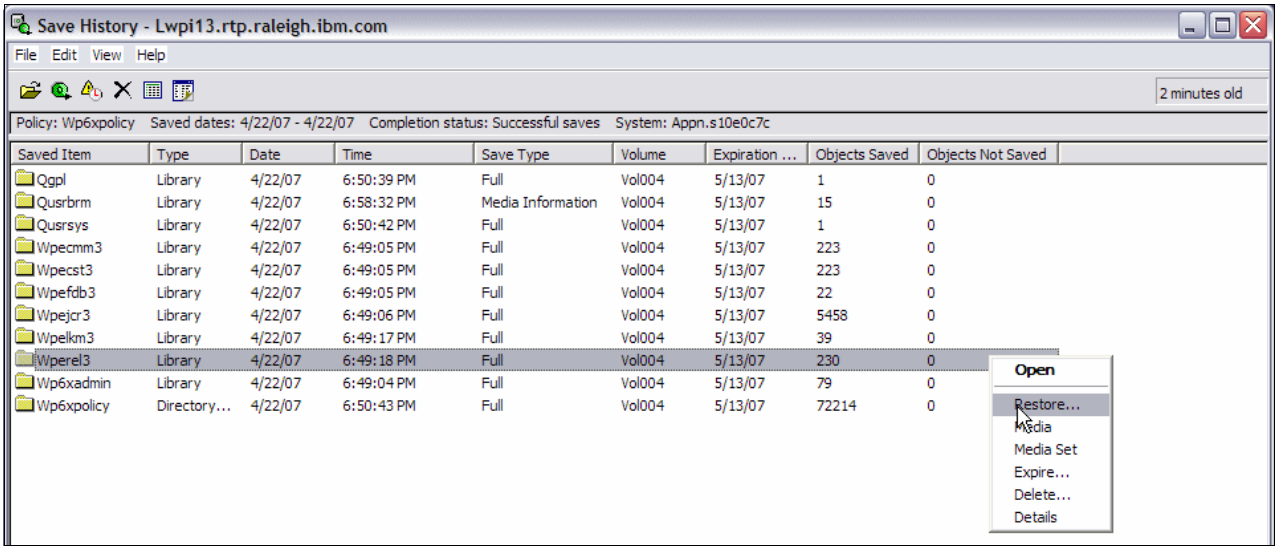

Save History - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
2 minutes old
Policy: Wp6xpolicy Saved dates: 4/22/07 - 4/22/07 Completion status: Successful saves System: Appn.s10e0c7c
Saved Item Type Date Time Save Type Volume Expiration ... Objects Saved Objects Not Saved
Qgpl Library 4/22/07 6:50:39 PM Full Vol004 5/13/07 1 0
Qusrbrm Library 4/22/07 6:58:32 PM Media Information Vol004 5/13/07 15 0
Qusrsys Library 4/22/07 6:50:42 PM Full Vol004 5/13/07 1 0
Wpecmm3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 223 0
Wpecst3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 223 0
Wpefdb3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 22 0
Wpejcr3 Library 4/22/07 6:49:06 PM Full Vol004 5/13/07 5458 0
Wpelkm3 Library 4/22/07 6:49:17 PM Full Vol004 5/13/07 39 0
Wperel3 Library 4/22/07 6:49:18 PM Full Vol004 5/13/07 230 0
Wp6xadmin Library 4/22/07 6:49:04 PM Full Vol004 5/13/07 79 0
Wp6xpolicy Directory... 4/22/07 6:50:43 PM Full Vol004 5/13/07 72214 0
Open
Restore...
Media
Media Set
Expire...
Delete...
Details

Figure 6-75 Restoring one schema database

5. On the Restore - Welcome window (Figure 6-76), click **Next**.

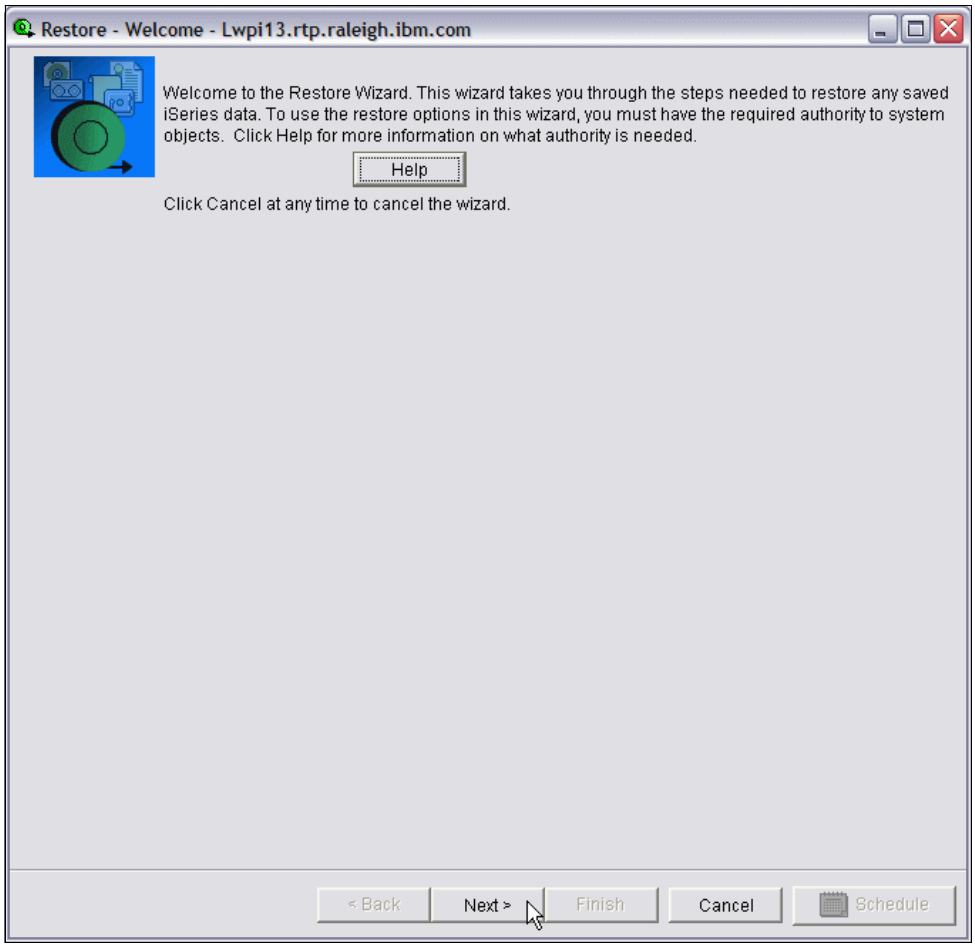

Restore - Welcome - Lwpi13.rtp.raleigh.ibm.com
Welcome to the Restore Wizard. This wizard takes you through the steps needed to restore any saved iSeries data. To use the restore options in this wizard, you must have the required authority to system objects. Click Help for more information on what authority is needed.
Help
Click Cancel at any time to cancel the wizard.
< Back
Next >
Finish
Cancel
Schedule

Figure 6-76 Restore wizard Welcome window

6. On the Restore Entire Save window (Figure 6-77), select **Restore entire selected save** and click **Next**.

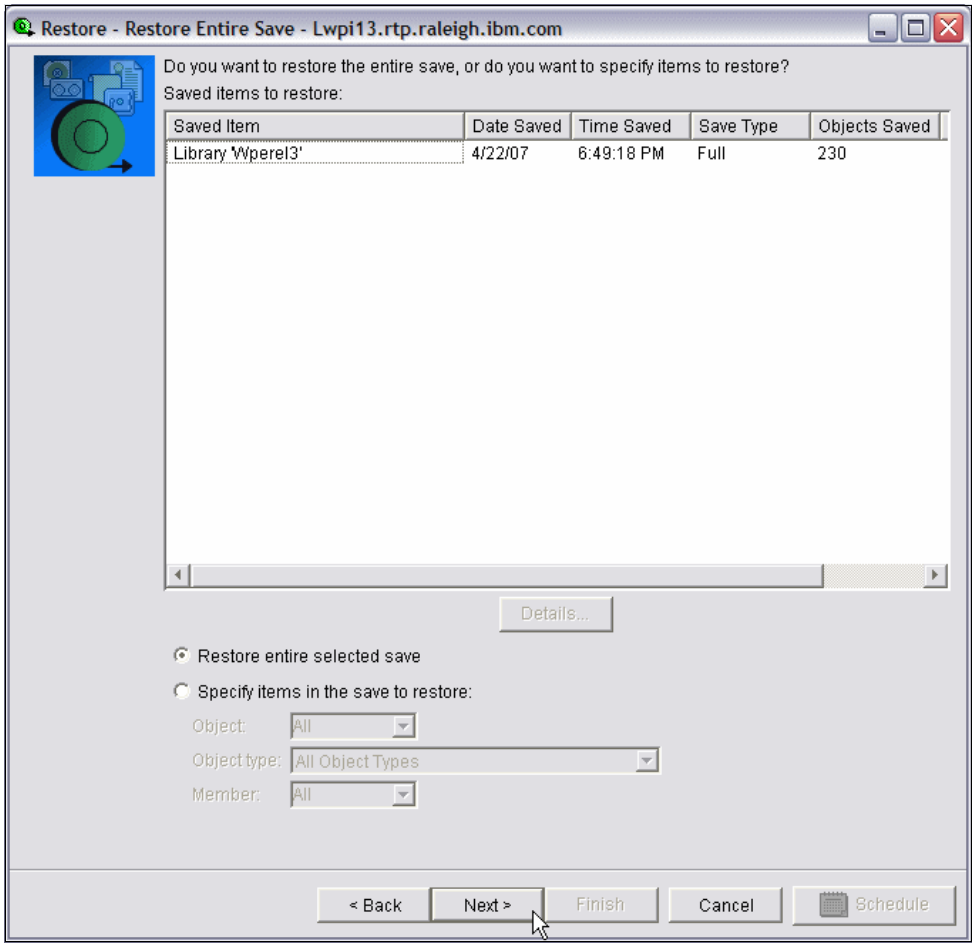


Figure 6-77 Specifying to restore entire selected save

7. On the Journaled Objects window (Figure 6-78), you can restore the data before the incident occurred. In Figure 6-78, we put a time to illustrate the point in time recovery times. We expect the journal changes to be applied up to the time we specified. Select **Apply journaled changes to a current date and time**. Remember that for the time you specify, the applied changes go as far as the receivers have data. Applying those changes to the current data and time is the easiest option. This way, the journal receivers apply all the changes that they have. Click **Next**.

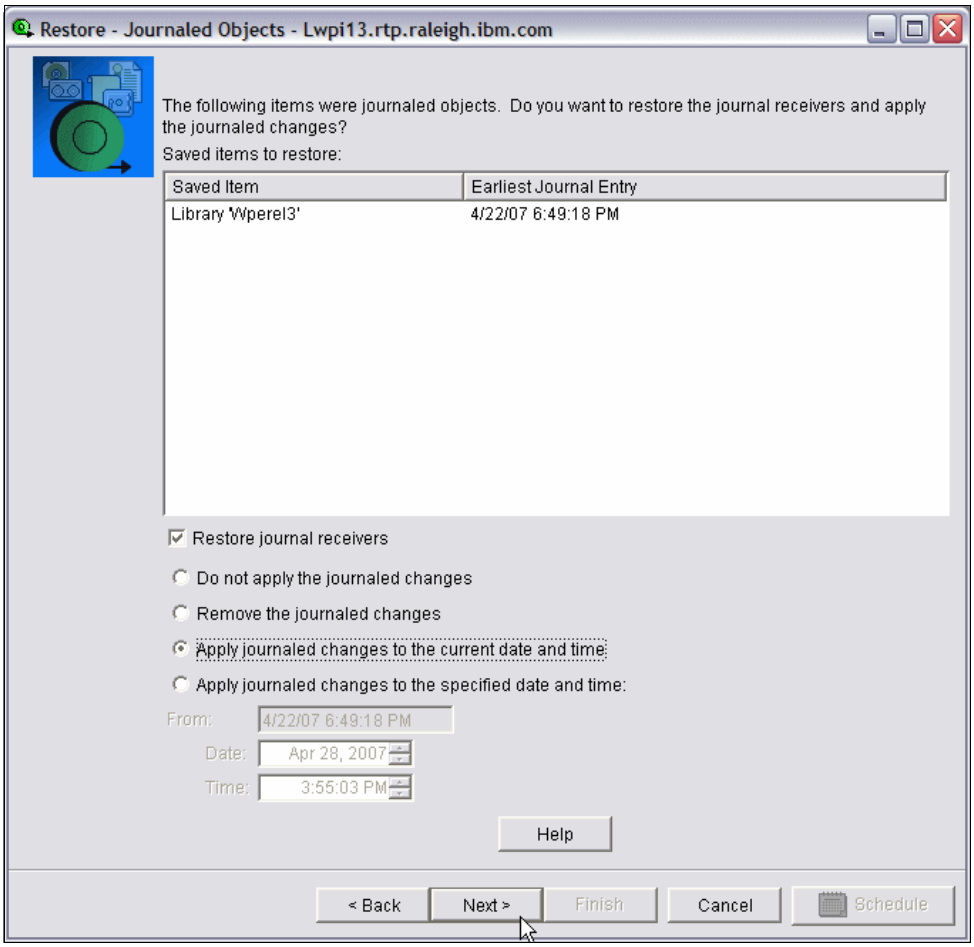


Figure 6-78 Restoring to current date and time

8. For our example, we want to restore to the same disk pool the data was saved in. The Restore To Same Disk Pool window (Figure 6-79) restores the object in a different disk pool. Select **Yes, restore to the same disk pool** and click **Next**.

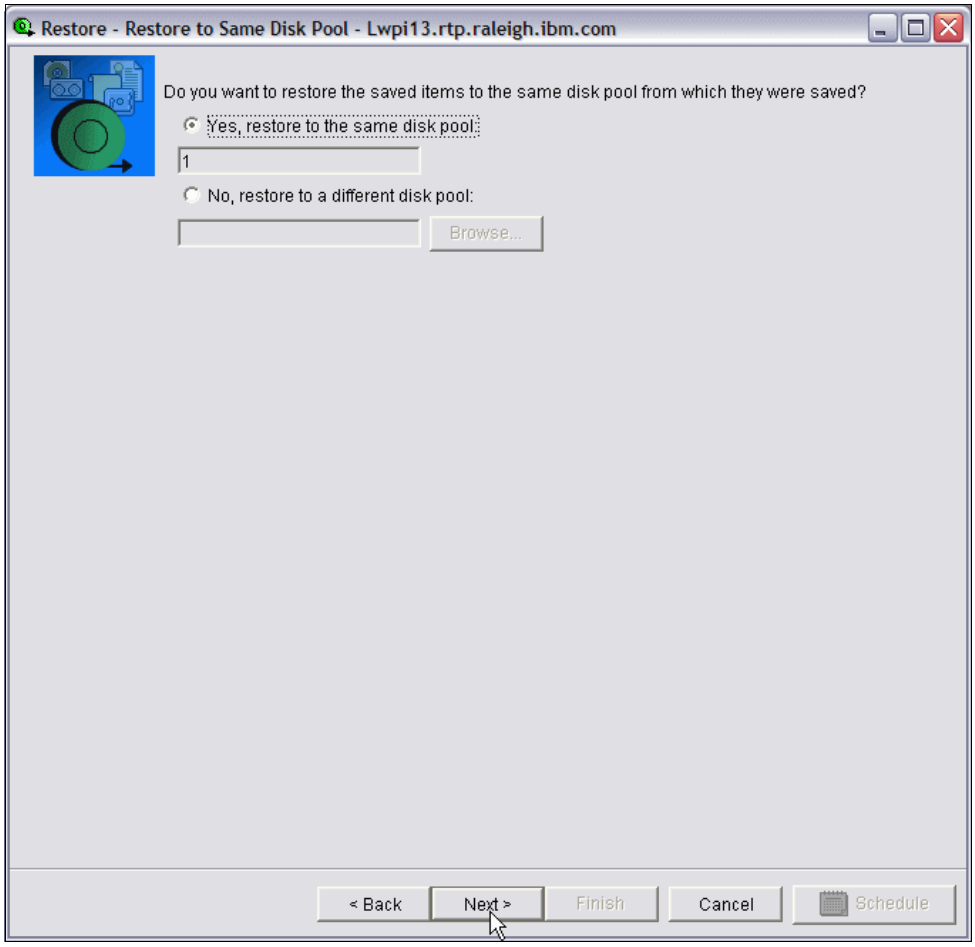

Restore - Restore to Same Disk Pool - Lwpi13.rtp.raleigh.ibm.com
Do you want to restore the saved items to the same disk pool from which they were saved?
Yes, restore to the same disk pool:
1
No, restore to a different disk pool:
Browse...
< Back
Next >
Finish
Cancel
Schedule

Figure 6-79 Restoring to the same disk pool

9. On the Use Save History Device window (Figure 6-80), you have the option of selecting the device to restore. Otherwise, let it select automatically. Click **Next**.

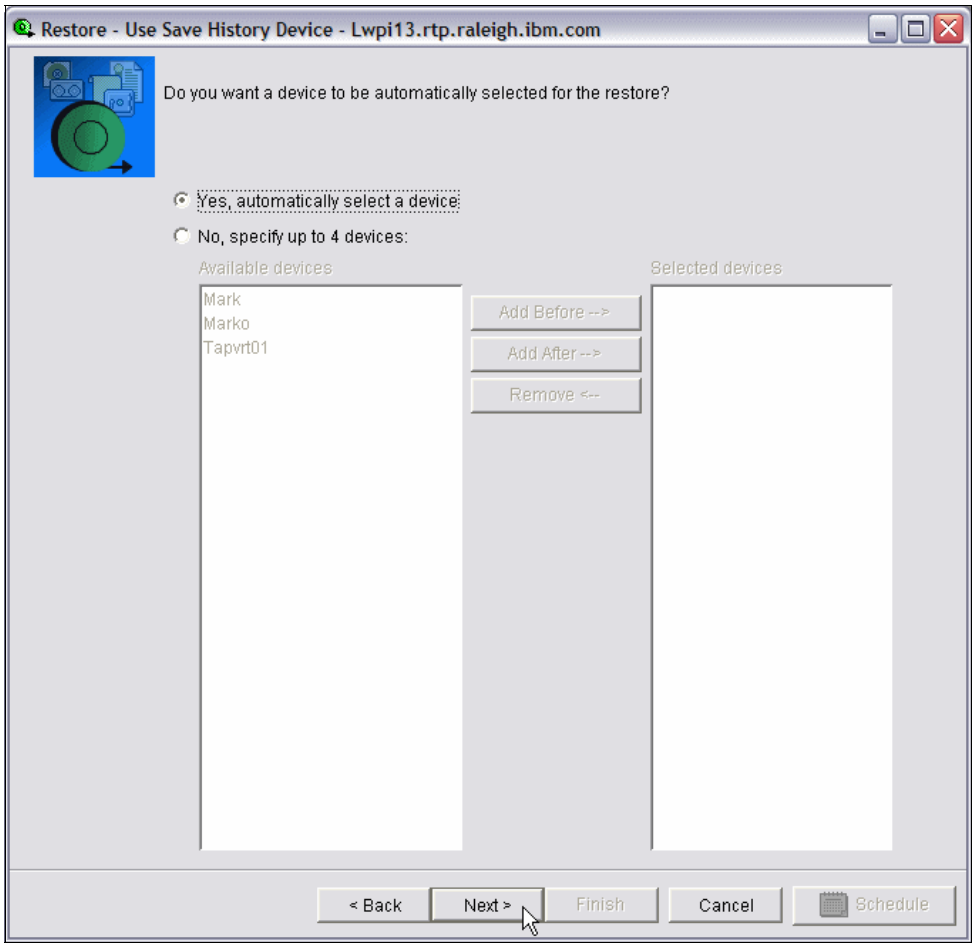


Figure 6-80 Automatically selecting a device for the restore

10. On the Summary window (Figure 6-81), you can inspect what you intend to restore. You can click **Details** see a list the files to be restored. Click **Advanced Options**.

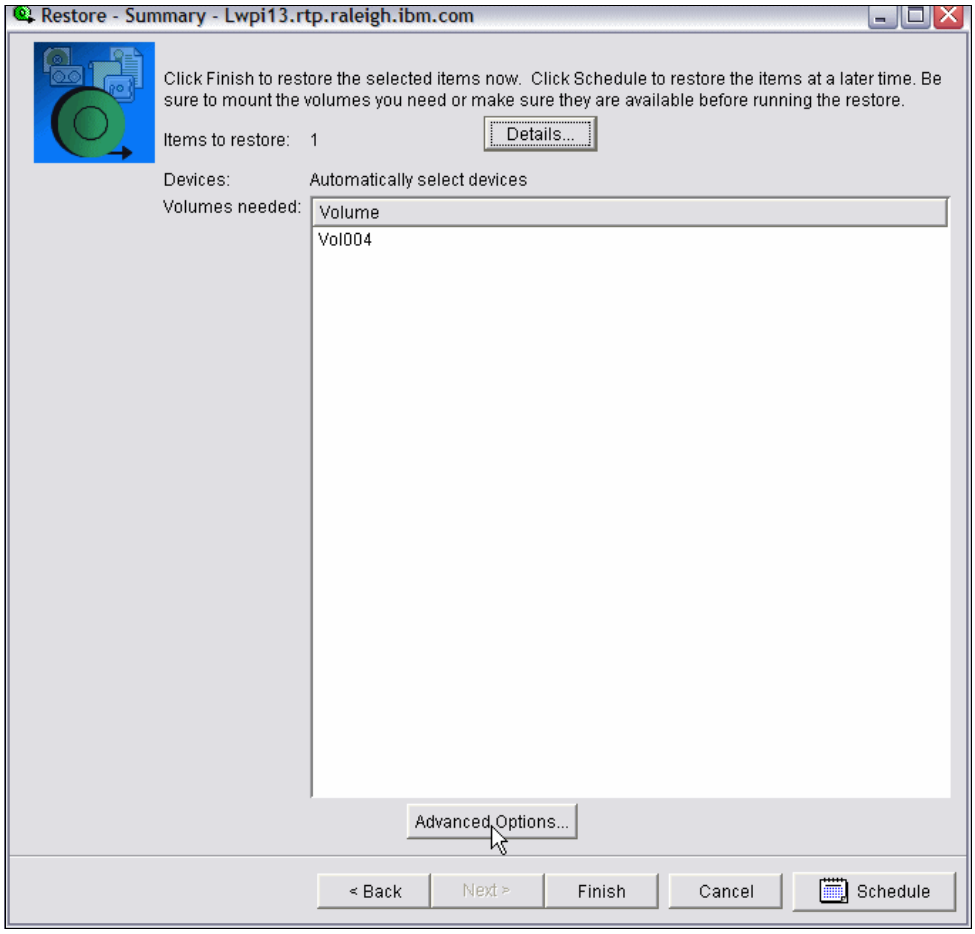

Restore - Summary - Lwpi13.rtp.raleigh.ibm.com
Click Finish to restore the selected items now. Click Schedule to restore the items at a later time. Be sure to mount the volumes you need or make sure they are available before running the restore.
Items to restore: 1
Details...
Devices: Automatically select devices
Volumes needed:
Volume
Vol004
Advanced Options...
< Back
Next >
Finish
Cancel
Schedule

Figure 6-81 Summary of the restore

11. The Restore - Advanced Options window (Figure 6-82) allows you to specify additional attributes to be applied to the restore operation. This is important if you are restoring over existing libraries. For the Database members to restore section, select **All members.** The Allow object differences section enables you to do the following:

   – Allows restore of a physical file with file level differences
   – Eliminates renaming of files on restore (for example, File0001, File0002)
   – Restores over existing files with file and member level differences

   Check the options as shown in Figure 6-82: **File level**, **Authorization list, Owner, Primary group**.

   You can specify the end of tape action to be applied after the restore operation completes in the **Device options** section. Click **OK**.

   Note: You *must* select certain non-default options (allowing file differences) in the Restore wizard to properly restore the libraries over existing ones. See the following article link on using ALWOBJDIF(*FILELVL) at:

   http://www-912.ibm.com/s_dir/slkbase.NSF/0/9b5f099dd280fb5186256a6b005d56a0?OpenDocument

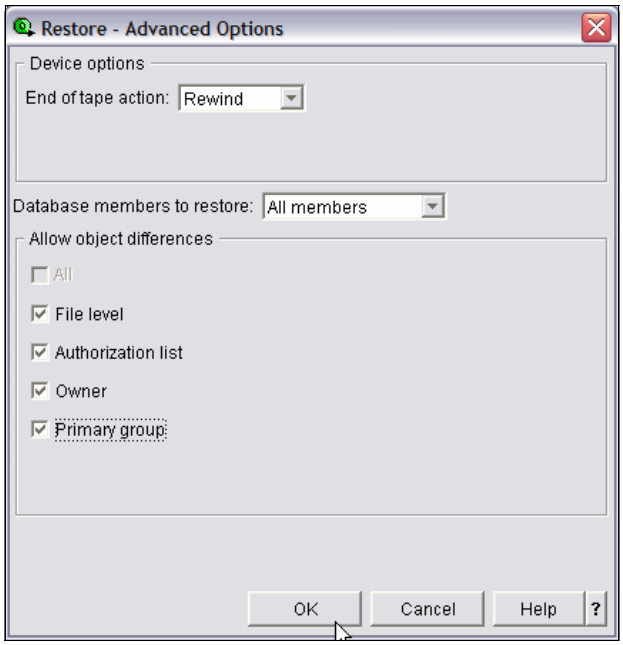


Figure 6-82 Selecting the advanced restore options

12. Back on the Summary window, click **Finish** to start the restore (Figure 6-83).

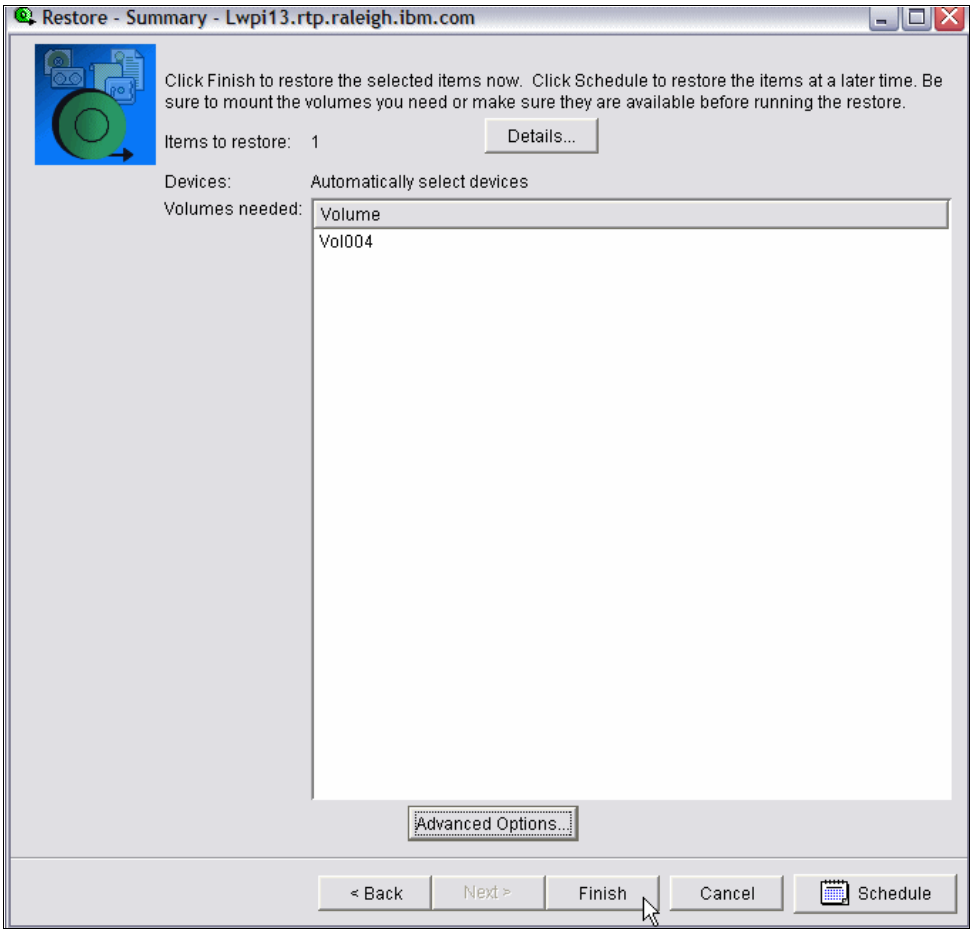

Restore - Summary - Lwpi13.rtp.raleigh.ibm.com
Click Finish to restore the selected items now. Click Schedule to restore the items at a later time. Be sure to mount the volumes you need or make sure they are available before running the restore.
Items to restore: 1
Details...
Devices: Automatically select devices
Volumes needed:
Volume
Vol004
Advanced Options...
< Back
Next >
Finish
Cancel
Schedule

Figure 6-83 Starting the restore

13. At this point, a connection is made to the Management Central system and the restore process starts.

Restoring the rest of the databases

Repeat the steps in “Restoring the RELEASE database” on page 307 to individually restore each of the following databases:

- CUSTOMIZATION database
- COMMUNITY database
- JCR database
- WMM database
- FEEDBACK database
- LIKEMINDS database

6.5.3 Restoring the HTTP server member object

Perform the following steps to restore the HTTP server member object:

1. Follow Steps 1 on page 307 to Step 3 on page 308 in the “Restoring the RELEASE database” on page 307.

2. The Save History window (Figure 6-84) shows the various folder, object, and directory lists that match the criteria you selected in the last step. Select the **Qusrsys** library and double-click it.

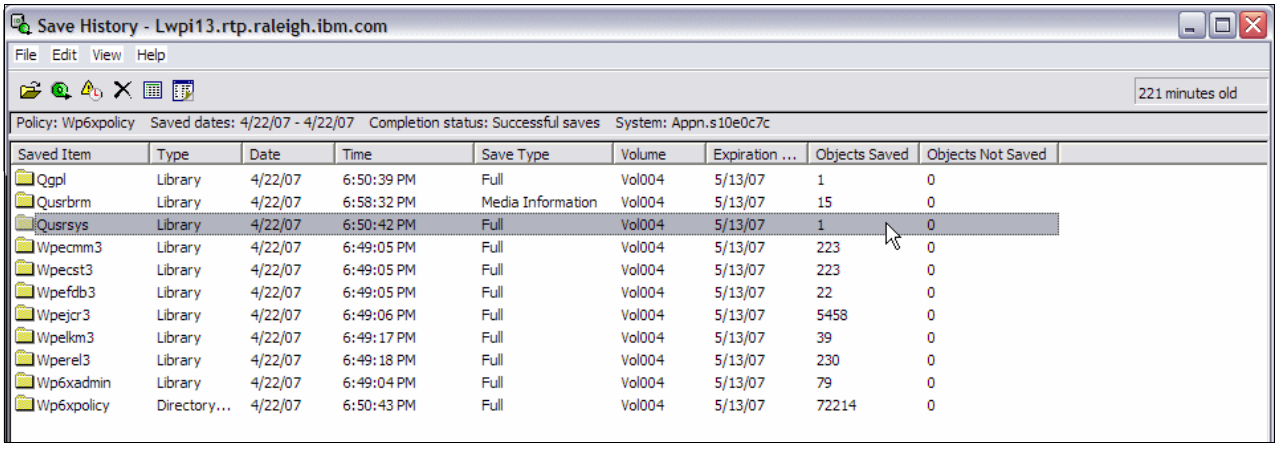

Save History - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
221 minutes old
Policy: Wp6xpolicy Saved dates: 4/22/07 - 4/22/07 Completion status: Successful saves System: Appn.s10e0c7c
Saved Item | Type | Date | Time | Save Type | Volume | Expiration ... | Objects Saved | Objects Not Saved
Qgpl | Library | 4/22/07 | 6:50:39 PM | Full | Vol004 | 5/13/07 | 1 | 0
Qusrbrm | Library | 4/22/07 | 6:58:32 PM | Media Information | Vol004 | 5/13/07 | 15 | 0
Qusrsys | Library | 4/22/07 | 6:50:42 PM | Full | Vol004 | 5/13/07 | 1 | 0
Wpecmm3 | Library | 4/22/07 | 6:49:05 PM | Full | Vol004 | 5/13/07 | 223 | 0
Wpecst3 | Library | 4/22/07 | 6:49:05 PM | Full | Vol004 | 5/13/07 | 223 | 0
Wpefdb3 | Library | 4/22/07 | 6:49:05 PM | Full | Vol004 | 5/13/07 | 22 | 0
Wpejcr3 | Library | 4/22/07 | 6:49:06 PM | Full | Vol004 | 5/13/07 | 5458 | 0
Wpelkm3 | Library | 4/22/07 | 6:49:17 PM | Full | Vol004 | 5/13/07 | 39 | 0
Wperel3 | Library | 4/22/07 | 6:49:18 PM | Full | Vol004 | 5/13/07 | 230 | 0
Wp6xadmin | Library | 4/22/07 | 6:49:04 PM | Full | Vol004 | 5/13/07 | 79 | 0
Wp6xpolicy | Directory... | 4/22/07 | 6:50:43 PM | Full | Vol004 | 5/13/07 | 72214 | 0

Figure 6-84 Selecting the Qusrsys folder

3. Double-click the **QATMHINSTC** file (Figure 6-85).

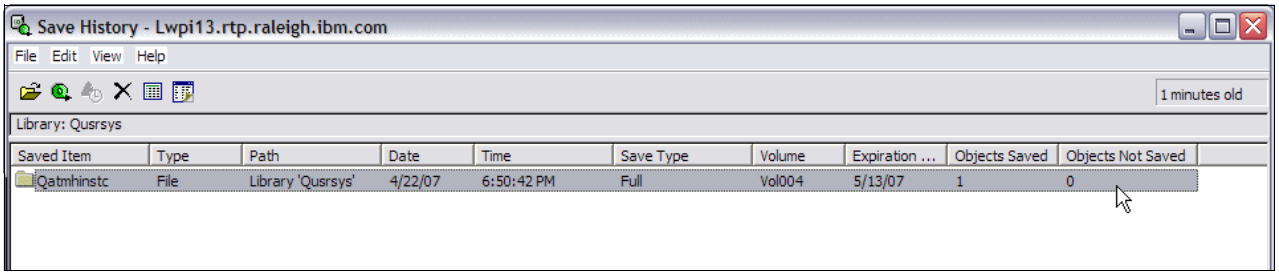

Save History - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
1 minutes old
Library: Qusrsys
Saved Item | Type | Path | Date | Time | Save Type | Volume | Expiration ... | Objects Saved | Objects Not Saved
Qatmhinstc | File | Library 'Qusrsys' | 4/22/07 | 6:50:42 PM | Full | Vol004 | 5/13/07 | 1 | 0

Figure 6-85 Selecting the qatmhinstc file

4. You see the HTTP member that matches the name of the your Web server. Right-click the object, **Wp6xweb** in our example, and select **Restore** (Figure 6-86).

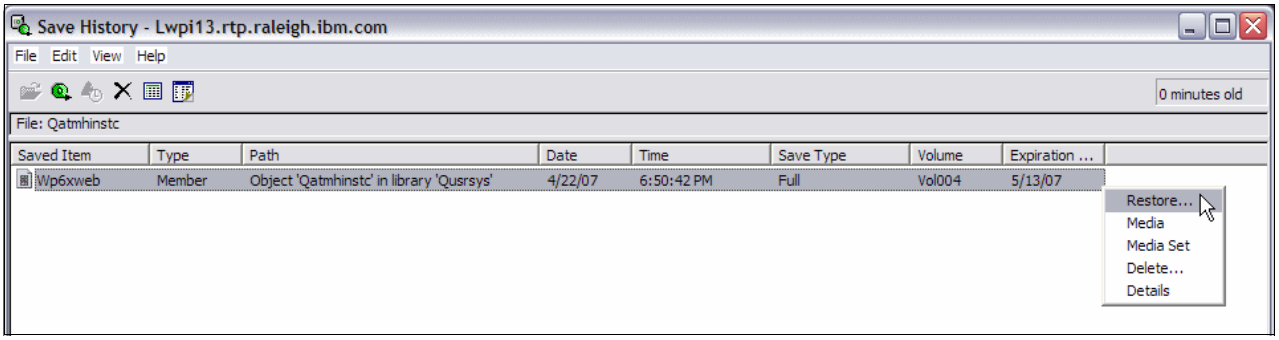

Save History - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
0 minutes old
File: Qatmhinstc
Saved Item | Type | Path | Date | Time | Save Type | Volume | Expiration ...
Wp6xweb | Member | Object 'Qatmhinstc' in library 'Qusrsys' | 4/22/07 | 6:50:42 PM | Full | Vol004 | 5/13/07
Restore...
Media
Media Set
Delete...
Details

Figure 6-86 Restoring the HTTP server member object

5. Follow Step 5 on page 310 to Step 13 on page 317 in the “Restoring the RELEASE database” on page 307 section to complete the restoration of the HTTP server member object.

6.5.4 Restoring user profile and security data

In the section, you restore the save file that was used to save all the user profiles and security data. Remember that while we only need the database owner user profile, we need to save all user profiles with the Save Security Data (SAVSECDTA) CL command because this was the simplest way to achieve our goal. For the restore process, you can restore the save file and then later use the PostExpressRestore.sh script to restore the needed profile. Perform the following steps:

1. Follow Steps 1 on page 307 to Step 3 on page 308 in the “Restoring the RELEASE database” on page 307.
2. The Save History window (Figure 6-87) shows the various folder, object, and directory lists that match the criteria you selected in the last step. Select the **Qgpl** library and double-click it.

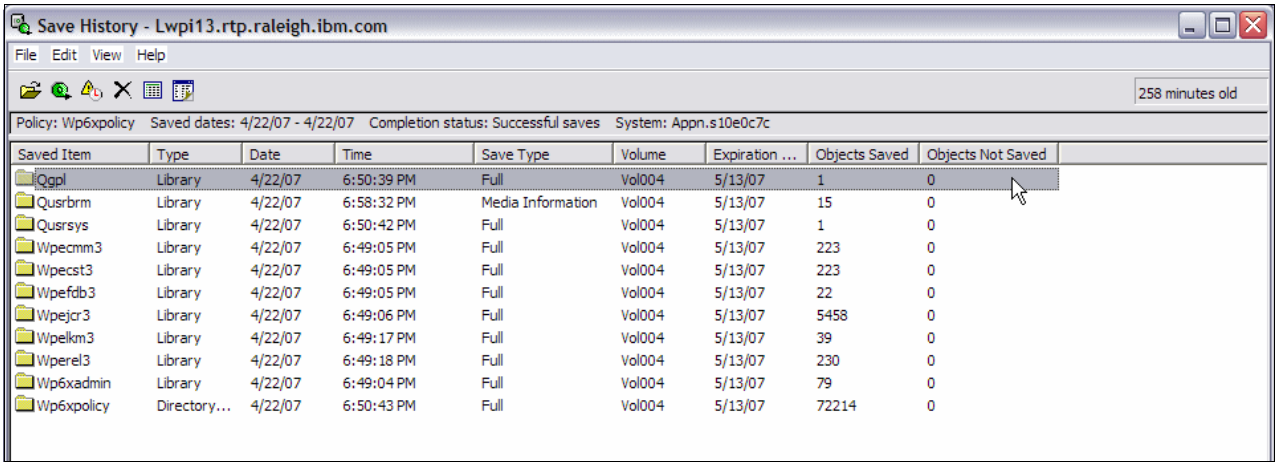

Save History - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
258 minutes old
Policy: Wp6xpolicy Saved dates: 4/22/07 - 4/22/07 Completion status: Successful saves System: Appn.s10e0c7c
Saved Item Type Date Time Save Type Volume Expiration ... Objects Saved Objects Not Saved
Qgpl Library 4/22/07 6:50:39 PM Full Vol004 5/13/07 1 0
Qusrbrm Library 4/22/07 6:58:32 PM Media Information Vol004 5/13/07 15 0
Qusrsys Library 4/22/07 6:50:42 PM Full Vol004 5/13/07 1 0
Wpecmm3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 223 0
Wpecst3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 223 0
Wpefdb3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 22 0
Wpejcr3 Library 4/22/07 6:49:06 PM Full Vol004 5/13/07 5458 0
Wpelkm3 Library 4/22/07 6:49:17 PM Full Vol004 5/13/07 39 0
Wperel3 Library 4/22/07 6:49:18 PM Full Vol004 5/13/07 230 0
Wp6xadmin Library 4/22/07 6:49:04 PM Full Vol004 5/13/07 79 0
Wp6xpolicy Directory... 4/22/07 6:50:43 PM Full Vol004 5/13/07 72214 0

Figure 6-87 Selecting the Qgpl folder

3. You see the save file for the user profiles. Right-click the object, **userprofs** in our example, and select **Restore** (Figure 6-88).

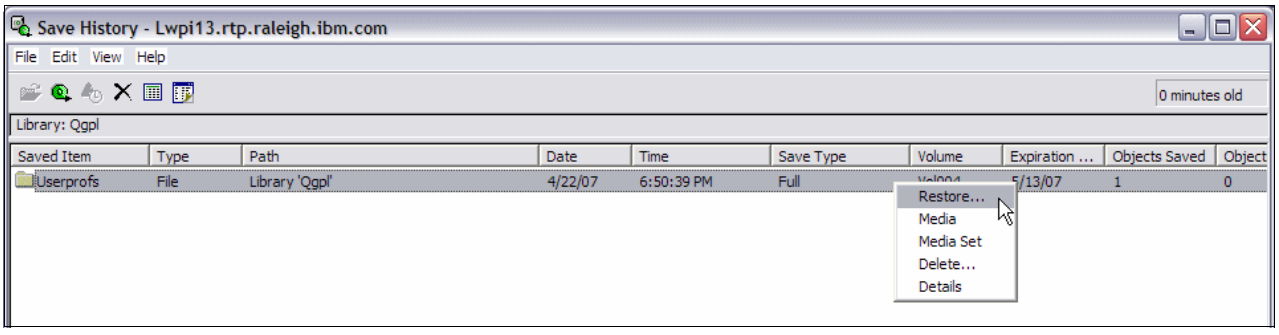

Save History - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
0 minutes old
Library: Qgpl
Saved Item Type Path Date Time Save Type Volume Expiration ... Objects Saved Object
Userprofs File Library 'Qgpl' 4/22/07 6:50:39 PM Full 5/13/07 1 0
Restore...
Media
Media Set
Delete...
Details

Figure 6-88 Selecting the user profiles save file

4. Follow Step 5 on page 310 to Step 13 on page 317 in the “Restoring the RELEASE database” on page 307 section to complete the restoration of the user profile and security data.

6.5.5 Restoring the integrated file system files

In this section, we show how to restore only i5/OS integrated file system files from the full save. Perform the following steps:

1. Follow Steps 1 on page 307 to Step 3 on page 308 in the “Restoring the RELEASE database” on page 307.
2. The Save History window (Figure 6-89) shows the various folder, object, and directory lists that match the criteria you selected in the last step. Select the list of files you want to restore. In our example, we want to restore the directory list of `wp6xpolicy`.

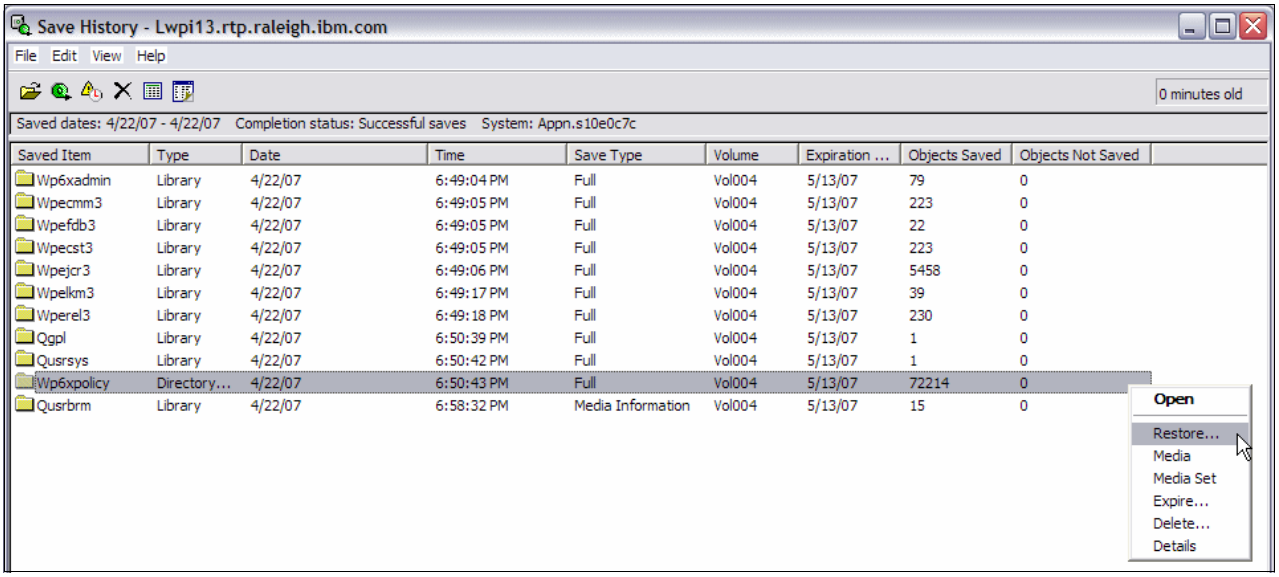

Save History - Lwpi13.rtp.raleigh.ibm.com
File Edit View Help
0 minutes old
Saved dates: 4/22/07 - 4/22/07 Completion status: Successful saves System: Appn.s10e0c7c
Saved Item Type Date Time Save Type Volume Expiration ... Objects Saved Objects Not Saved
Wp6xadmin Library 4/22/07 6:49:04 PM Full Vol004 5/13/07 79 0
Wpecmm3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 223 0
Wpefdb3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 22 0
Wpecst3 Library 4/22/07 6:49:05 PM Full Vol004 5/13/07 223 0
Wpejcr3 Library 4/22/07 6:49:06 PM Full Vol004 5/13/07 5458 0
Wpelkm3 Library 4/22/07 6:49:17 PM Full Vol004 5/13/07 39 0
Wperel3 Library 4/22/07 6:49:18 PM Full Vol004 5/13/07 230 0
Qgpl Library 4/22/07 6:50:39 PM Full Vol004 5/13/07 1 0
Qusrsys Library 4/22/07 6:50:42 PM Full Vol004 5/13/07 1 0
Wp6xpolicy Directory... 4/22/07 6:50:43 PM Full Vol004 5/13/07 72214 0
Qusrbrm Library 4/22/07 6:58:32 PM Media Information Vol004 5/13/07 15 0
Open
Restore...
Media
Media Set
Expire...
Delete...
Details

Figure 6-89 Selecting the directory list you want to restore

3. On the Restore wizard Welcome window (Figure 6-90), click **Next**.

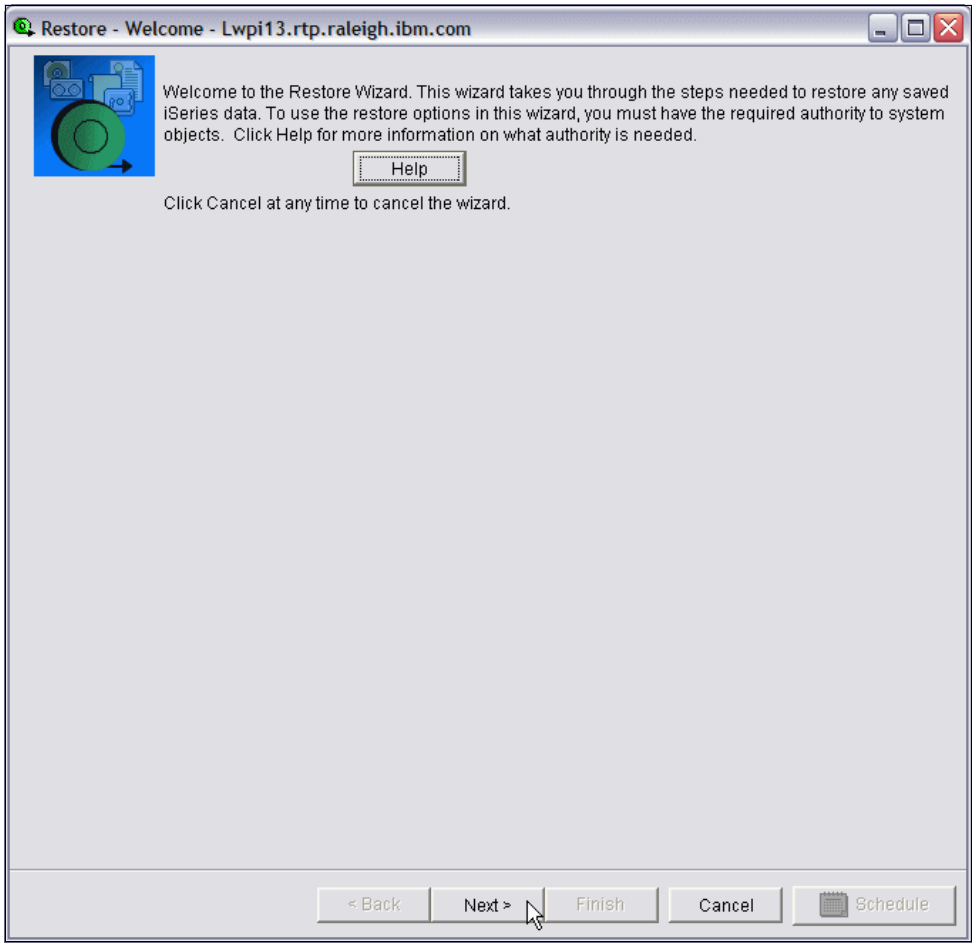

Restore - Welcome - Lwpi13.rtp.raleigh.ibm.com
Welcome to the Restore Wizard. This wizard takes you through the steps needed to restore any saved iSeries data. To use the restore options in this wizard, you must have the required authority to system objects. Click Help for more information on what authority is needed.
Help
Click Cancel at any time to cancel the wizard.
< Back
Next >
Finish
Cancel
Schedule

Figure 6-90 Restore wizard Welcome window

4. On the Restore Entire Save window (Figure 6-91), select **Restore entire selected save** and click **Next**.

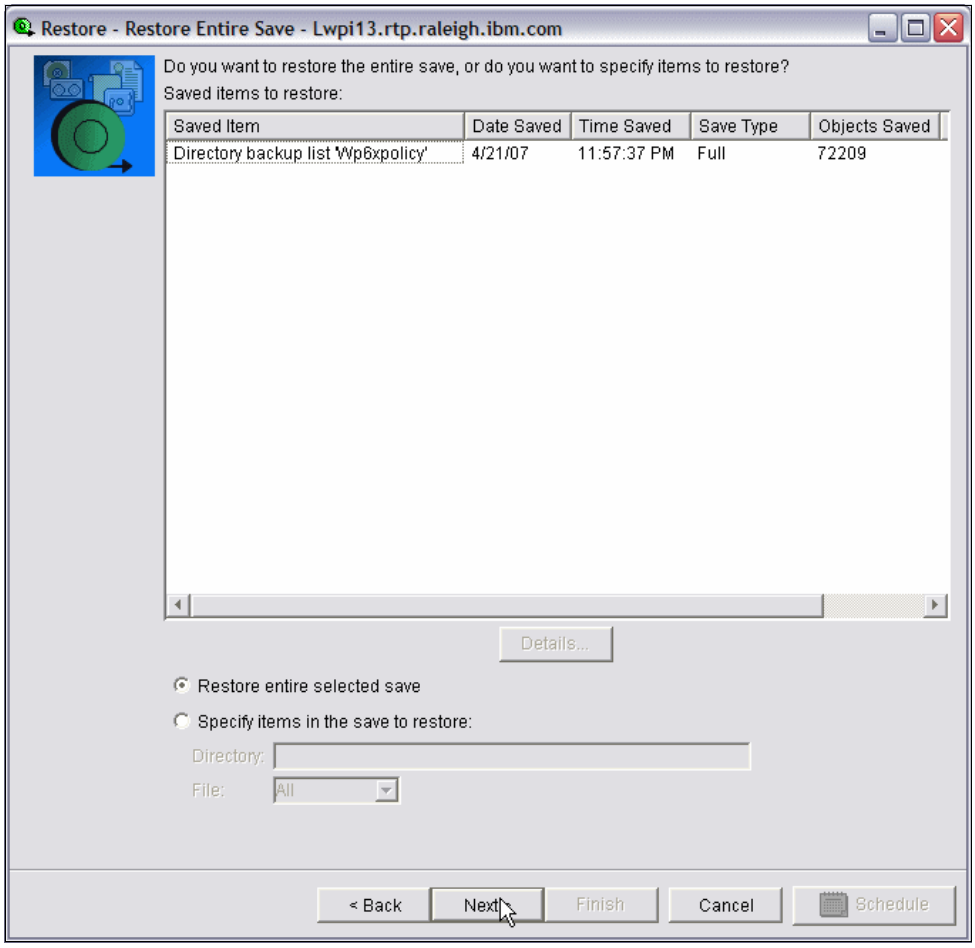


Figure 6-91 Restoring the directory list

5. On the Restore Directory window (Figure 6-92), select **Restore directory and all files** and select the check box next to **Include subdirectories**. Click **Next**.

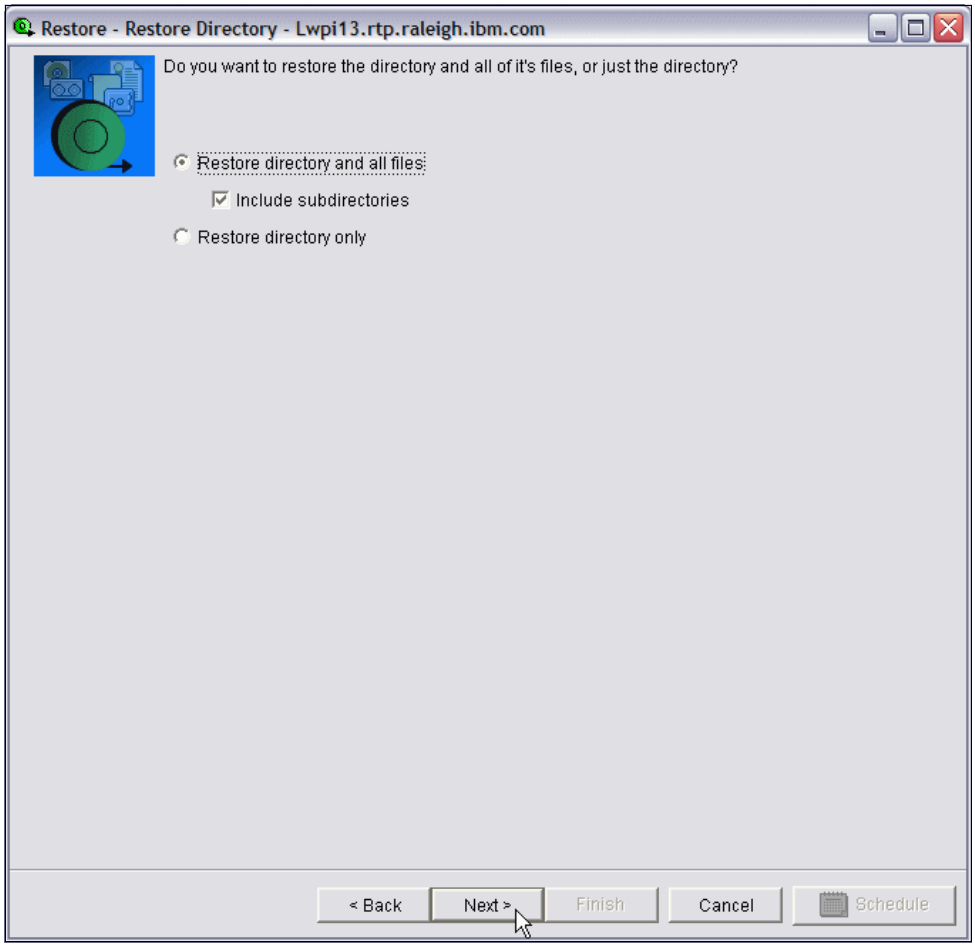

Restore - Restore Directory - Lwpi13.rtp.raleigh.ibm.com
Do you want to restore the directory and all of it's files, or just the directory?
Restore directory and all files
Include subdirectories
Restore directory only
< Back
Next >
Finish
Cancel
Schedule

Figure 6-92 Specifying to restore all directories

6. On the Use Save History Device window (Figure 6-93), you have the option of selecting the device to restore. Otherwise, let it select automatically. Click **Next**.

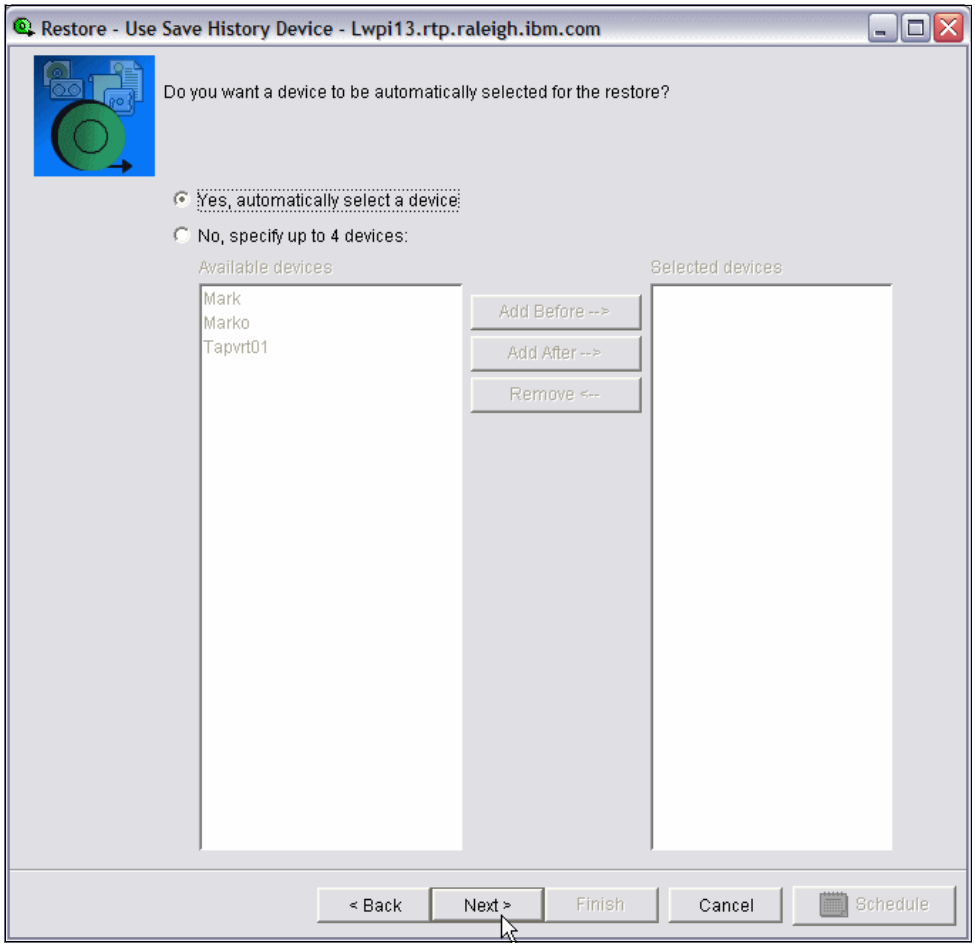


Figure 6-93 Automatically selecting a device for the restore

7. On the Summary window (Figure 6-94), you can inspect what you intend to restore. You can click **Details** to see a list of the files to be restored. Click **Advanced Options**.

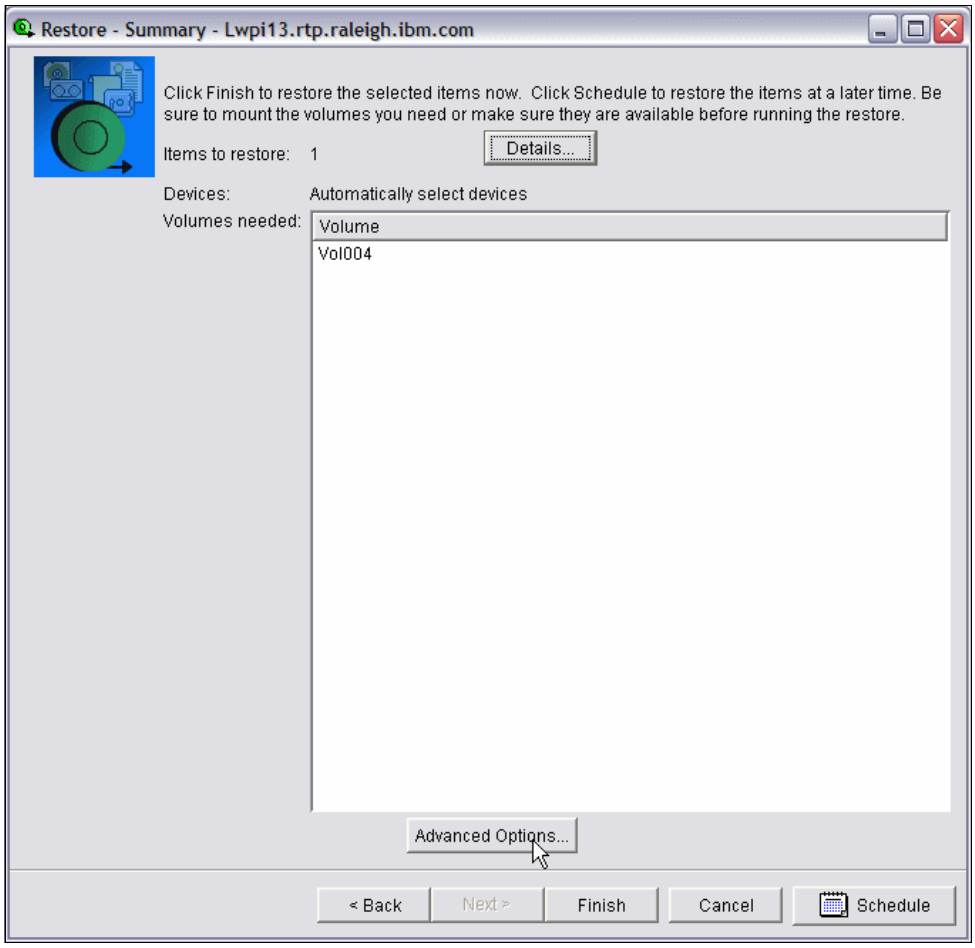

Restore - Summary - Lwpi13.rtp.raleigh.ibm.com
Click Finish to restore the selected items now. Click Schedule to restore the items at a later time. Be sure to mount the volumes you need or make sure they are available before running the restore.
Items to restore: 1
Details...
Devices: Automatically select devices
Volumes needed:
Volume
Vol004
Advanced Options...
< Back
Next >
Finish
Cancel
Schedule

Figure 6-94 Summary of the restore

8. The Restore - Advanced Options window (Figure 6-95) allows you to specify additional attributes to be applied to the restore operation. This is important if you are restoring over already existing files. Select **All** in the Allow object differences section. Click **OK**.

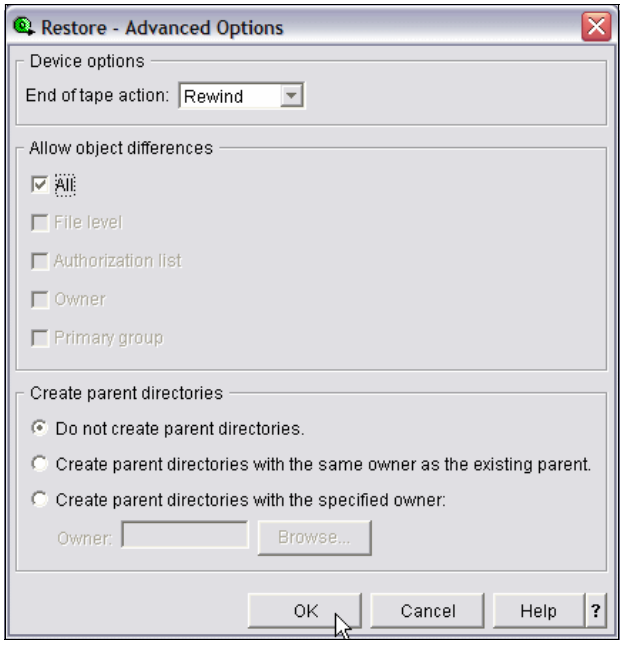


Figure 6-95 Selecting the advanced restore options

9. Back on the Summary window, click **Finish** to start the restore process (Figure 6-96).

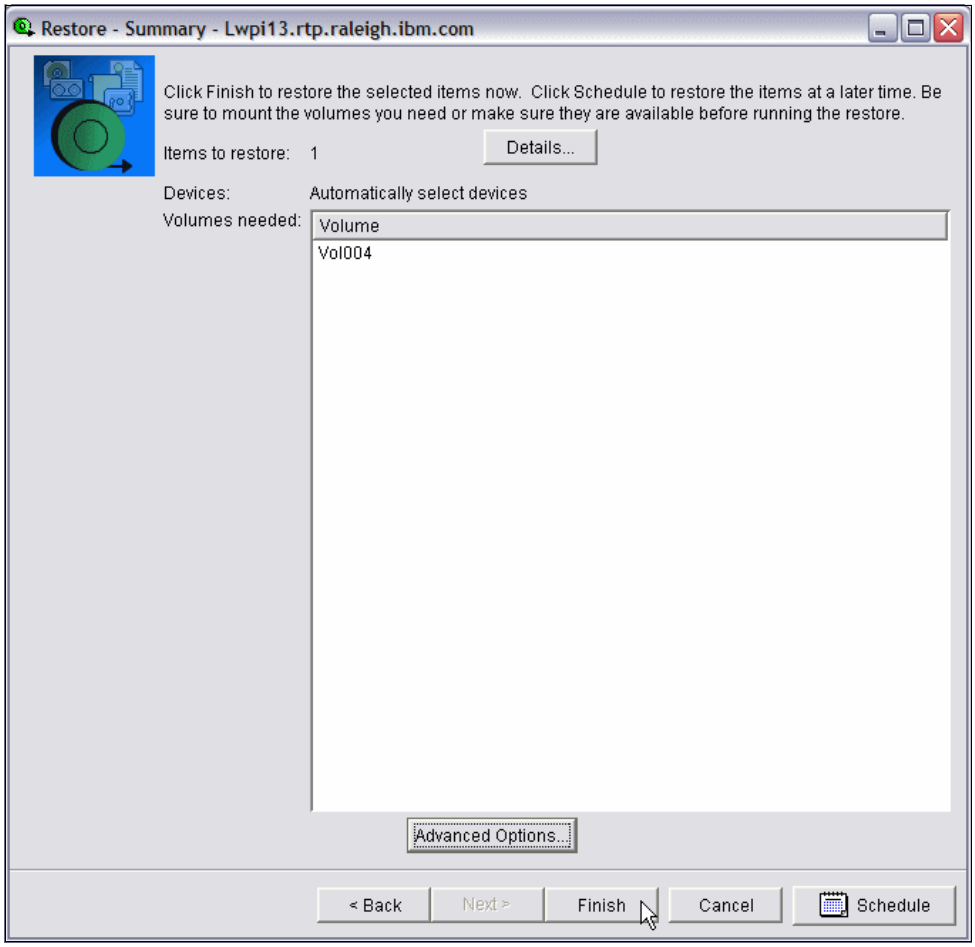

Restore - Summary - Lwpi13.rtp.raleigh.ibm.com
Click Finish to restore the selected items now. Click Schedule to restore the items at a later time. Be sure to mount the volumes you need or make sure they are available before running the restore.
Items to restore: 1
Details...
Devices: Automatically select devices
Volumes needed:
Volume
Vol004
Advanced Options...
< Back
Next >
Finish
Cancel
Schedule

Figure 6-96 Start the restore

a. At this point, a connection is made to the Management Central system and the restore process starts.

6.5.6 Running the PostExpressRestore.sh script

The PostExpressRestore.sh script restores the user profiles that corresponds to the portal profile's Database Administrator. It also restores or grants the necessary authorities for that profile. Lastly, the script restores the private authorities of QTMHHTTP and QEJBSVR for the objects restored. See 6.4.3, "Running the PostExpressRestore.sh script" on page 304 for details about how to run this command.

6.6 Using the BRMS commands for backup and restore

Some users are more comfortable with the i5/OS command line or 5250 emulation session. This section provides an example of saving and restoring a WebSphere Portal Express server with a backup policy. We assume that the backup policy has already been created with a BRMS client. See 6.3.1, "Creating a backup policy using the Backup Policy wizard" on page 247 for details.

6.6.1 Running a backup with a policy using i5/OS commands

Perform the following steps to run a backup with a policy using i5/OS commands:

1. From a 5250 emulation session, log on to your system.
2. From an i5/OS command line, access the BRMS environment by entering the following command and pressing Enter:

   ```
   GO BRMS
   ```

3. On the Backup Recovery and Media Services for iSeries menu, type option `2` (Backup) and press Enter (Figure 6-97).

```
BRMS            Backup Recovery and Media Services for iSeries
                                                        System:   LWPI13
Select one of the following:

     1. Media management
     2. Backup
     3. Archive
     4. Recovery
     5. Migration

    10. Scheduling
    11. Policy administration
    12. Reports

    20. Start console monitor




Selection or command
===>   2

F3=Exit   F4=Prompt   F9=Retrieve   F10=Commands   F12=Cancel   F13=Functions
(C) COPYRIGHT IBM CORP. 1998, 2006. ALL RIGHTS RESERVED.
```

Figure 6-97 Backup Recovery and Media Services for iSeries menu

4. On the Backup menu (Figure 6-98), type option 2 (Perform backup) and press Enter.

```
BRMBKU                              Backup
                                                        System:   LWPI13
Select one of the following:

     1. Backup planning
     2. Perform backup
     3. Display backup activity
     4. Start console monitor




Selection or command
===> 2

F3=Exit   F4=Prompt   F9=Retrieve   F10=Commands   F12=Cancel   F13=Functions
```

Figure 6-98 Backup menu

5. On the Start Backup using BRM (STRBKUBRM) command prompt (Figure 6-99), enter the control group name appropriate for your environment. Normally, the control group name is the same as the policy. We also want to run the backup policy in batch mode and immediately. For our example, we enter the following parameters:
   - Control group: WP6XPOLICY
   - Schedule time: *IMMED
   - Submit to batch: *YES

   Press Enter.

```
                Start Backup using BRM (STRBKUBRM)

Type choices, press Enter.

Control group  . . . . . .  WP6XPOLICY    *BKUGRP, *SYSGRP, *SYSTEM...
Schedule time  . . . . . .   *IMMED        hhmm, *IMMED
Submit to batch  . . . . .   *YES          *YES, *CONSOLE, *CTLSBS, *NO
Starting sequence:
  Number . . . . . .  . .    *FIRST        1-9999, *FIRST
  Library  . . . . . .  .    *FIRST        Name, *FIRST
Append to media  . . . . .   *CTLGRPATR    *CTLGRPATR, *BKUPCY, *NO...









                                                                   Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 6-99 Start Backup using BRM (STRBKUBRM) command prompt

6. More options for the Start Backup using BRM (STRBKUBRM) command prompt are shown (Figure 6-100). Review the entries and press Enter to start the backup.

```
                     Start Backup using BRM (STRBKUBRM)

Type choices, press Enter.

Control group  . . . . . . . . . > WP6XPOLICY    *BKUGRP, *SYSGRP, *SYSTEM...
Schedule time  . . . . . . . . .   *IMMED        hhmm, *IMMED
Submit to batch  . . . . . . . .   *YES          *YES, *CONSOLE, *CTLSBS, *NO
Starting sequence:
  Number . . . . . . . . . . . .   *FIRST        1-9999, *FIRST
  Library  . . . . . . . . . . .   *FIRST        Name, *FIRST
Append to media  . . . . . . . .   *CTLGRPATR    *CTLGRPATR, *BKUPCY, *NO...
Job description  . . . . . . . .   *USRPRF       Name, *USRPRF
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Job queue  . . . . . . . . . . .   *JOBD         Name, *JOBD
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Activity . . . . . . . . . . . .   *CTLGRPATR    *CTLGRPATR, *FULL, *INCR
Retention:
  Retention type . . . . . . . .   *CTLGRPATR    *CTLGRPATR, *DAYS, *PERM
  Retain media . . . . . . . . .   35            1-9999
Omits  . . . . . . . . . . . . .   *PROCESS      *PROCESS, *IGNORE
                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 6-100 Start Backup using BRM (STRBKUBRM) command prompt, more options

7. At this point, the backup starts. You can review the backup job using the Work with Active Jobs (WRKACTJOB) command.
8. On the Work with Active Job display (Figure 6-101), locate the backup job. It is usually the same name as the backup policy. In our example, it is `WP6XPOLICY`. Type option `5` (Work with) next to the job and press Enter.

```
                      Work with Active Jobs                     LWPI13
                                                             04/29/07  02:35:53
CPU %:     1.8     Elapsed time:   04:42:46     Active jobs:   394

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect ...
                    Current
Opt  Subsystem/Job  User        Type  CPU %  Function        Status
     QBATCH         QSYS        SBS      .0                 DEQW
 5     WP6XPOLICY   MOWUSUA     BCH      .0  CMD-STRBKUBRM   RUN
     QCMN           QSYS        SBS      .0                 DEQW
     QCTL           QSYS        SBS      .0                 DEQW
     QHTTPSVR       QSYS        SBS      .0                 DEQW
       ADMIN        QTMHHTTP    BCH      .0  PGM-QZHBMAIN    SIGW
       ADMIN        QTMHHTTP    BCI      .0  PGM-QZSRLOG     SIGW
       ADMIN        QTMHHTTP    BCH      .0  PGM-QLWISVR     JVAW
       ADMIN        QTMHHTTP    BCI      .0  PGM-QZSRHTTP    SIGW
                                                                More...
Parameters or command
===>
F3=Exit   F5=Refresh       F7=Find      F10=Restart statistics
F11=Display elapsed data   F12=Cancel   F23=More options   F24=More keys
```

Figure 6-101 Work with Active Jobs display

9. On the Work with Job menu for the backup job (Figure 6-102), type option 10 (Display job log, if active, on job queue, or pending) and press Enter to work with the job log of the restore job.

```
                        Work with Job
                                                            System:   LWPI13
Job:   WP6XPOLICY     User:   MOWUSUA        Number:   165279

Select one of the following:

     1. Display job status attributes
     2. Display job definition attributes
     3. Display job run attributes, if active
     4. Work with spooled files

    10. Display job log, if active, on job queue, or pending
    11. Display call stack, if active
    12. Work with locks, if active
    13. Display library list, if active
    14. Display open files, if active
    15. Display file overrides, if active
    16. Display commitment control status, if active
                                                                        More...
Selection or command
===> 10

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
```

Figure 6-102 Work with Job menu for the backup job

10. The job log for the backup job is displayed (Figure 6-103). Press F10 and then F5 to show more of the job log. Use the Page Down key to continue reviewing the job log.

Tip: You can also use the Display Log for BRM (DSPLOGBRM) CL command to review the progress of the backup.

```
                          Display All Messages
                                                              System:   LWPI13
Job . . :   WP6XPOLICY    User . . :   MOWUSUA       Number . . . :   165279

    Job 165279/MOWUSUA/WP6XPOLICY started on 04/29/07 at 02:35:47 in subsystem
      QBATCH in QSYS. Job entered system on 04/29/07 at 02:35:47.
    Job 165279/MOWUSUA/WP6XPOLICY submitted.
 >> STRBKUBRM CTLGRP(WP6XPOLICY) SCDTIME(*IMMED) SBMJOB(*NO) STRSEQ(*FIRST *FI
    RST) APPEND(*CTLGRPATR) ACTIVITY(*CTLGRPATR) RETENTION(*CTLGRPATR 0035) OM
    ITS(*PROCESS)
    Begin processing for control group WP6XPOLICY type *BKU.
    Printer device PRT01 not found. Output queue changed to QPRINT in library
      QGPL.









                                                                        Bottom
Press Enter to continue.

F3=Exit    F5=Refresh    F12=Cancel    F17=Top    F18=Bottom
```

Figure 6-103 Reviewing the job log of the backup job

6.6.2 Restoring with a policy using i5/OS commands

Perform the following steps to run a restore with a backup policy using i5/OS commands:

1. From a 5250 emulation session, log on to your system.
2. Run the PreExpressRestore.sh script to clean up the existing portal profile. Enter the following command on the i5/OS command line:

   ```
   STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/PreExpressRestore.sh -p
   <profilename>')
   ```

   For our example, this is:

   ```
   STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/PreExpressRestore.sh -p
   wp6xserver')
   ```

3. From an i5/OS command line, access the BRMS environment by entering the following command and pressing Enter:

   ```
   GO BRMS
   ```

4. On the Backup Recovery and Media Services for iSeries menu (Figure 6-104), type option 4 (Recovery) and press Enter.

```
BRMS            Backup Recovery and Media Services for iSeries
                                                              System:   LWPI13
Select one of the following:

     1. Media management
     2. Backup
     3. Archive
     4. Recovery
     5. Migration

    10. Scheduling
    11. Policy administration
    12. Reports

    20. Start console monitor


Selection or command
===> 4

F3=Exit   F4=Prompt   F9=Retrieve   F10=Commands   F12=Cancel   F13=Functions
(C) COPYRIGHT IBM CORP. 1998, 2006. ALL RIGHTS RESERVED.
```

Figure 6-104 Backup Recovery and Media Services for iSeries menu

5. On the Recovery menu, type option 2 (Perform recovery) and press Enter (Figure 6-105).

```
BRMRCY                              Recovery
                                                      System:   LWPI13
Select one of the following:

     1. Recovery planning
     2. Perform recovery
     3. Display recovery activity









Selection or command
===> 2

F3=Exit   F4=Prompt   F9=Retrieve   F10=Commands   F12=Cancel   F13=Functions
(C) COPYRIGHT IBM CORP. 1998, 2006. ALL RIGHTS RESERVED.
```

Figure 6-105 Recovery menu

6. On the Perform Recovery menu (Figure 6-106), since we want to restore data saved with a backup policy, type option 3 (Recover control group) and press Enter.

```
BRMRCYOPT                     Perform Recovery
                                                          System:   LWPI13
Select one of the following:

     1. Recover system
     2. Recover auxiliary storage pool (ASP)
     3. Recover control group
     4. Recover library
     5. Work with media information
     6. Work with saved objects
     7. Work with saved folders
     8. Work with saved spooled files
     9. Work with saved link information



Selection or command
===> 3

F3=Exit   F4=Prompt   F9=Retrieve   F10=Commands   F12=Cancel   F13=Functions
```

Figure 6-106 Perform recovery menu

7. On the Start Recovery using BRM (STRRCYBRM) command prompt display (Figure 6-107), review the parameters. Look at the backup dates from which you want to restore. You can press the F10 key to review the rest of the parameters. When you are finished reviewing, press Enter.

```
               Start Recovery using BRM (STRRCYBRM)

Type choices, press Enter.

Option . . . . . . . . . . . . . > *CTLGRP       *SYSTEM, *ALLDLO, *ALLUSR...
Action . . . . . . . . . . . . . > *RESTORE      *REPORT, *RESTORE
Time period for recovery:
  Start time and date:
  Beginning time . . . . . . . .   *AVAIL        Time, *AVAIL
  Beginning date . . . . . . . .   04/22/07      Date, *CURRENT, *BEGIN
  End time and date:
  Ending time  . . . . . . . . .   *AVAIL        Time, *AVAIL
  Ending date  . . . . . . . . .   04/22/07      Date, *CURRENT, *END
Use save files . . . . . . . . .   *YES          *YES, *NO
Use TSM  . . . . . . . . . . . .   *YES          *YES, *NO
Control group selection:
  Control group  . . . . . . . .   *SELECT       Name, *SELECT, *NONE...
  Sequence number  . . . . . . .                 1-99
              + for more values

                                                                      More...
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

Figure 6-107 Start Recovery using BRM (STRRCYBRM) command prompt

8. On the Select and Sequence Control Groups display (Figure 6-108), select the control group that corresponds to the backup policy. In our example, type an option `1` next to the backup policy called `WP6XPOLICY` and press Enter.

```
                  Select and Sequence Control Groups              LWPI13

Type sequence number (1-99), press Enter.

         Control
  Seq    Group         Text

         *NONE         *NONE
         *BKUGRP       Backs up all user data
         *SYSGRP       Backs up all system data
         *SYSTEM       Backs up the entire system
         EXPRESS       backup policy
         EXPRESS60     express60
         MONTHLY       *NONE
         QLTSDOM00     LWPI13LDAP
         QLTSSVR       Online backup of all Lotus servers
         SAVSECDTA     TEST
    1    WP6XPOLICY    This is an online backup policy forWP6XSERVER

                                                                    Bottom

F3=Exit    F9=Review backup plan    F12=Cancel
```

Figure 6-108 Selecting the backup policy

9. On the Select Recovery Items display (Figure 6-109), select the various items you want to restore. In our case, we want to restore all the items saved for the specific dates we specified in Figure 6-107 on page 336. Type an option `1` (Select) next to all the items you want to restore. Press the F9 (Recovery defaults), which allows you to inspect or change the restore options.

```
                          Select Recovery Items                    LWPI13

                                              Select action  . . . . . : *ALL
                                              Select volume  . . . . . :
Type options, press Enter.
  1=Select   4=Remove   5=Display   7=Specify object

   Saved        Save     Save   Save   Parallel Volume    File        Expire
pt Item         Date     Time   Type   Devices  Serial    Sequence    Date
1  WP6XADMIN   4/22/07 18:49:04 *FULL           VOL004          111    5/13/07
1  WPECMM3     4/22/07 18:49:05 *FULL           VOL004          112    5/13/07
1  WPECST3     4/22/07 18:49:05 *FULL           VOL004          114    5/13/07
1  WPEFDB3     4/22/07 18:49:05 *FULL           VOL004          113    5/13/07
1  WPEJCR3     4/22/07 18:49:06 *FULL           VOL004          115    5/13/07
1  WPELKM3     4/22/07 18:49:17 *FULL           VOL004          116    5/13/07
1  WPEREL3     4/22/07 18:49:18 *FULL           VOL004          117    5/13/07
1  QGPL        4/22/07 18:50:39 *FULL           VOL004          118    5/13/07
1  QUSRSYS     4/22/07 18:50:42 *FULL           VOL004          119    5/13/07
1  WP6XPOLICY  4/22/07 18:50:43 *FULL           VOL004          120    5/13/07

                                                                      Bottom
F3=Exit   F5=Refresh   F9=Recovery defaults   F11=Object View
F12=Cancel   F14=Submit to batch   F16=Select
```

Figure 6-109 Selecting the items to restore

10. The Restore Command Defaults display (Figure 6-110) allows you to specify additional attributes to be applied to the restore operation. The Allow object differences parameter is the most relevant because it enables you to do the following:

   – Allows restore of a physical file with file level differences
   – Eliminates renaming of files on restore (for example, `File0001`, `File0002`)
   – Restores over existing files with file/member level differences

   Fill in the relevant parameters appropriate for your environment. When you are done, press the Page Down key to access additional restore parameters.

> **Note:** You *must* select certain non-default options (allowing file differences) in the Restore wizard to properly restore libraries over existing ones. See the following article link on using ALWOBJDIF(*FILELVL) at:
>
> `http://www-912.ibm.com/s_dir/slkbase.NSF/0/9b5f099dd280fb5186256a6b005d56a0?OpenDocument`

```
                      Restore Command Defaults

Type information, press Enter.

 Device  . . . . . . . . . . . . . . . TAP01      Name, *MEDCLS

 Parallel device resources:
   Minimum resources. . . . . . . .  *SAV         1-32, *NONE, *AVAIL
   Maximum resources. . . . . . . .               1-32, *AVAIL, *MIN
 End of tape option  . . . . . . . . *REWIND     *REWIND, *LEAVE, *UNLOAD
 Option  . . . . . . . . . . . . . . *ALL        *ALL, *NEW, *OLD, *FREE
 Data base member option . . . . . . *ALL        *MATCH, *ALL, *NEW, *OLD
 Restore spooled file data . . . . . *NONE       *NONE, *NEW
 Allow object differences  . . . . . *FILELVL
                                     *OWNER      *NONE, *ALL, *AUTL,
                                     *PGP        *FILELVL, *OWNER, *PGP


                                                                      More...
 F12=Cancel
```

Figure 6-110 Changing the restore options

11. The second panel of the Restore Command Defaults display (Figure 6-111) allows you to change options to restore journal receivers and point in time recovery. For our example, we specify the following parameters:
    - Restore journal receivers = *YES
    - Apply option =*APPLY
    - Ending date = *CURRENT
    - Ending time = *CURRENT

    Press Enter.

> **Note:** Depending on your recovery objectives, consider saving all changed journal receivers periodically. During the event of disaster recovery, if all required journal receivers were saved periodically, then BRMS can perform recovery up to the last commitment boundary based on last saved journal receivers. Journal receivers contain database update information that can replay to perform point in time recovery. See the IBM Redpaper *Improve Whole System Backups with the New Save-While-Active Function*, REDP-7200, at:
>
> http://www.redbooks.ibm.com/abstracts/redp7200.html

```
                      Restore Command Defaults

Type information, press Enter.

 Restore to library  . . . . . *SAVLIB     Name, *SAVLIB
 Auxiliary storage pool  . . . . . *SAVASP     Name, *SAVASP, 1-32...
 Document name generation  . . . . . *SAME       *SAME, *NEW
 System resource management  . . . . *ALL        *ALL, *NONE, *HDW, *TRA
 Apply journaled changes:
   Restore journal receivers . . . . *YES        *YES, *NO
   Apply option  . . . . . *APPLY      *NONE, *APPLY, *REMOVE
     Ending date . . . . . *CURRENT    Date, *CURRENT
     Ending time . . . . . *CURRENT    Time, *CURRENT
 Lotus point-in-time:
   Ending date . . . . . *CURRENT    Date, *CURRENT, *FULL
   Ending time . . . . . *CURRENT    Time, *CURRENT, *FULL
 Create parent directories . . . . . *NO         *NO, *YES
   Parent directories owner  . . . . *PARENT     Name, *PARENT



                                                                      Bottom
 F12=Cancel
```

Figure 6-111 Restoring journal receivers

12. You are returned to the Select Recovery Items display (Figure 6-112). Submitting the restore in batch mode allows a job to run more efficiently. Press F14 (Shift+F2) to submit the job in batch mode.

```
                          Select Recovery Items                    LWPI13

                                              Select action  . . . . . : *ALL
                                              Select volume  . . . . . :
Type options, press Enter.
  1=Select   4=Remove   5=Display   7=Specify object

   Saved        Save     Save   Save   Parallel Volume    File        Expire
pt Item         Date     Time   Type   Devices  Serial    Sequence    Date
1  WP6XADMIN   4/22/07 18:49:04 *FULL           VOL004          111    5/13/07
1  WPECMM3     4/22/07 18:49:05 *FULL           VOL004          112    5/13/07
1  WPECST3     4/22/07 18:49:05 *FULL           VOL004          114    5/13/07
1  WPEFDB3     4/22/07 18:49:05 *FULL           VOL004          113    5/13/07
1  WPEJCR3     4/22/07 18:49:06 *FULL           VOL004          115    5/13/07
1  WPELKM3     4/22/07 18:49:17 *FULL           VOL004          116    5/13/07
1  WPEREL3     4/22/07 18:49:18 *FULL           VOL004          117    5/13/07
1  QGPL        4/22/07 18:50:39 *FULL           VOL004          118    5/13/07
1  QUSRSYS     4/22/07 18:50:42 *FULL           VOL004          119    5/13/07
1  WP6XPOLICY  4/22/07 18:50:43 *FULL           VOL004          120    5/13/07

                                                                  Bottom
F3=Exit   F5=Refresh   F9=Recovery defaults   F11=Object View
F12=Cancel   F14=Submit to batch   F16=Select
```

Figure 6-112 Using F14 to submit job as a batch job

13. On the Submit Job (SBMJOB) display (Figure 6-113), change the parameters as necessary. Also note the name of the restore job, QBRMRCY, because you might need to review the job log. You can use the F10 key to review additional parameters. Press Enter to start the restore process in batch mode.

```
                              Submit Job (SBMJOB)

Type choices, press Enter.

Job name . . . . . . . . . . . . > QBRMRCY       Name, *JOBD
Job description  . . . . . . . .   *USRPRF       Name, *USRPRF
  Library  . . . . . . . . . . .                  Name, *LIBL, *CURLIB
Job queue  . . . . . . . . . . .   *JOBD         Name, *JOBD
  Library  . . . . . . . . . . .                  Name, *LIBL, *CURLIB
Job priority (on JOBQ) . . . . .   *JOBD         1-9, *JOBD
Output priority (on OUTQ)  . . .   *JOBD         1-9, *JOBD
Print device . . . . . . . . . .   *CURRENT      Name, *CURRENT, *USRPRF...
Output queue . . . . . . . . . .   *CURRENT      Name, *CURRENT, *USRPRF...
  Library  . . . . . . . . . . .                  Name, *LIBL, *CURLIB



                                                                        More...
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

Figure 6-113 Submitting the restore job in batch mode

14. At this point, the job has been submitted to batch mode and might be running. Use the Work with Active Jobs (WRKACTJOB) command to review the job log.

15. In the Work with Active Job display, locate the restore job. In this case, it is QBRMRCY. Type option 5 (Work with) next to the job and press Enter (Figure 6-114).

```
                        Work with Active Jobs                    LWPI13
                                                              04/29/07  01:03:14
CPU %:      .8     Elapsed time:   03:10:07     Active jobs:   373

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect ...
                     Current
Opt  Subsystem/Job   User        Type  CPU %  Function        Status
     QBATCH          QSYS        SBS      .0                  DEQW
5      QBRMRCY       MOWUSUA     BCH      .0  PGM-Q1AC2RCY    RUN
     QCMN            QSYS        SBS      .0                  DEQW
     QCTL            QSYS        SBS      .0                  DEQW
     QHTTPSVR        QSYS        SBS      .0                  DEQW
       ADMIN         QTMHHTTP    BCH      .0  PGM-QZHBMAIN    SIGW
       ADMIN         QTMHHTTP    BCI      .0  PGM-QZSRLOG     SIGW
       ADMIN         QTMHHTTP    BCH      .0  PGM-QLWISVR     JVAW
       ADMIN         QTMHHTTP    BCI      .0  PGM-QZSRHTTP    SIGW
                                                                More...
Parameters or command
===>
F3=Exit   F5=Refresh       F7=Find      F10=Restart statistics
F11=Display elapsed data   F12=Cancel   F23=More options   F24=More keys
```

Figure 6-114 Locating the QBRMRCY job

16. On the Work with Job display, type option 10 (Display job log, if active, on job queue, or pending) and press Enter to work with the job log of the restore job (Figure 6-115).

```
                              Work with Job
                                                              System:   LWPI13
Job:   QBRMRCY        User:   MOWUSUA        Number:   164963

Select one of the following:

     1. Display job status attributes
     2. Display job definition attributes
     3. Display job run attributes, if active
     4. Work with spooled files

    10. Display job log, if active, on job queue, or pending
    11. Display call stack, if active
    12. Work with locks, if active
    13. Display library list, if active
    14. Display open files, if active
    15. Display file overrides, if active
    16. Display commitment control status, if active
                                                                          More...
Selection or command
===> 10

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
```

Figure 6-115 Accessing the restore job log

17. The job log is displayed. Press F10 and then F5 to show more of the job log (Figure 6-116). Use the Page Down key to continue reviewing the job log.

> **Tip:** You can also use the Display Log for BRM (DSPLOGBRM) CL command to review the progress of the restore.

```
                Display All Messages
                                                              System:   LWPI13
Job . . :   QBRMRCY       User . . :   MOWUSUA       Number . . . :   164963

 >> CALL PGM(QBRM/Q1AC2RCY) PARM('STRRCYBRM' 'C' X'0001E3C1D7E5D9E3F0F14040404
    0404040404040404040404040404040404040404040404040404040404040E7' X'0002FFFD000
    0' '*REWIND' '*ALL' '*ALL' '*NONE' '*FILELVL*OWNER  *PGP' '*SAME' '*SAVLIB
    ' '00' '*ALL' '012716' '*LCL' ' ' ' ' '*NO' DFTDIROWN)
    Devices TAPVRT01 will be used for control group *N type *RCY.
    Output file QASRRSTO created in library QTEMP.
    Member QASRRSTO added to output file QASRRSTO in library QTEMP.
    QDFTOWN owns LIB WP6XADMIN in QSYS.
    QDFTOWN owns JRN QSQJRN in WP6XADMIN.
    Journal QSQJRN in WP6XADMIN restored
    QDFTOWN owns FILE WMMUSERREG in WP6XADMIN.
    QDFTOWN owns FILE WMMI110 in WP6XADMIN.
    QDFTOWN owns FILE WMMI105 in WP6XADMIN.
                                                                        More...
Press Enter to continue.

F3=Exit   F5=Refresh   F12=Cancel   F17=Top   F18=Bottom
```

Figure 6-116 Restore job log

18. Upon successful completion of the restore, run the PostExpressRestore.sh script. Enter the following command on the i5/OS command line:

    ```
    STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/PostExpressRestore.sh -p
    <profilename>')
    ```

    For our example, this is:

    ```
    STRQSH CMD('/QIBM/ProdData/PortalExpress/V6/Tools/PostExpressRestore.sh -p
    wp6xserver')
    ```

    Figure 6-117 shows a partial output of the command. Note that there is log generated in /tmp directory that you can review in addition to what is shown on the console.

```
  Starting Time is 021759

  /QIBM/ProdData/PortalExpress/V6/Tools/PostExpressRestore.sh -p wp6xserver

  Profile is wp6xserver
  The output will also be sent to /tmp/PostExpressrestore.sh_021759.log
  Http Folder: /www/wp6xweb
  WMM_SCHEMA : wp6xadmin
  RELEASE_SCHEMA : WPEREL3
  CUSTOMIZATION_SCHEMA :  WPECST3
  COMMUNITY_SCHEMA  : WPECMM3
  JCR_SCHEMA  : WPEJCR3
  FEEDBACK_SCHEMA  :  WPEFDB3
  LIKEMINDS_SCHEMA  :  WPELKM3
  CPC3712:  USRPRF WP6XADMIN restored.
  CPC3705:  1 user profiles restored at 04/29/07 02:19:31.
  CPC3706:  Private authorities restored for user profile WP6XADMIN.

===>

F3=Exit F4=End of File F6=Print F9=Retrieve F17=Top
F18=Bottom  F19=Left   F20=Right F21=User Window
```

Figure 6-117 Running the PostExpressRestore.sh script

A

Upgrading to WebSphere Portal Express V6.0.1

This appendix describes how to upgrade from WebSphere Portal Express Version 6.0.0.1 to Version 6.0.1 on i5/OS. If you are upgrading to version 6.0.1.1, see Technote 1270778 at the following Web site for instructions on how to perform that particular upgrade:

http://www.ibm.com/support/docview.wss?rs=688&uid=swg21270778

Important: While this document assumes you are already running WebSphere Portal Express V6.0.0.1, see 2.6, “Program temporary fixes” on page 32 to ensure you meet all the necessary software and group PTF requirements.

Keep the following recommendations in mind to ensure a smooth upgrade:

- Make sure all the necessary passwords in the wpconfig.properties and wpconfig_dbdomain.properties files are filled in. The upgrade is unnecessarily lengthy if any required passwords are missing.
- If you are using or have deployed custom themes, skins, or screens in your environment, make sure they are deployed in production mode. See *Deploying customized themes and skins* information in the WebSphere Portal Information Center available at the following Web site. While the installation process takes extra steps to save the existing wps.ear application, improperly deployed customer themes, skins, JSPs, and so on can prevent the portal server from being fully functional after the upgrade.

  http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp?topic=/com.ibm.wp.ent.doc/wps/dgn_dpycst.html
- If you do not have any customized screens in the wps.ear application, then you might want the installation process to implement all the new screen changes in the version 6.0.1 refresh pack. To do so, set the following parameter in the wpconfig.properties file:

  ```
  CopyWpsEarScreens=true
  ```

  If you do not set this parameter, existing screens are not replaced.

© Copyright IBM Corp. 2007. All rights reserved.

Preparing for the upgrade

Perform the following steps to prepare for an upgrade of a WebSphere Portal Express Version 6.0.0.1 to Version 6.0.1:

1. Make sure you are at least at the following WebSphere Application Server group PTF level:
   - For i5/OS V5R3: WebSphere PTF group SF99301 (level 21 or higher)
   - For i5/OS V5R4: PTF group SF99312 (level 11 or higher)

   As part of the WebSphere Application Server fix strategy, you need to run an update command after the group PTFs are applied to properly apply the fixes. See *Fix Pack Installation Instructions: WebSphere Application Server V6.0* in the WebSphere Portal Information Center at:

   `http://www.ibm.com/servers/eserver/iseries/software/websphere/wsappserver/services/fixpack60.html`

   The steps essentially boil down to the following, shortly after applying the group PTFs:

   a. End the QWAS6 subsystem if active: `ENDSBS SBS(QWAS6)`

   b. Start the host servers if they are not active: `STRHOSTSVR *ALL`

   c. Run the following update command:

   ```
   STRQSH
   CMD('/QIBM/ProdData/WebSphere/AppServer/V6/Base/updateinstaller/update')
   ```

2. Download the following files from the WebSphere Portal Product Support Web site. You will need your IBM user name and password.

   `http://www.ibm.com/software/genservers/portal/support`

   - PortalUpdateInstaller.zip
   - 6.0.1-WP-Multi-RP001.zip
   - 6.0.1-WP-WSASv6.0.2.17-IFPackage.zip

3. Extract and transfer the zip files to i5/OS:

   a. Start the QShell environment: `STRQSH`

   b. For the PortalUpdateInstaller.zip file:

      i. Create a folder called update in the /QIBM/ProdData/PortalExpress/V6 directory:

      ```
      mkdir /QIBM/ProdData/PortalExpress/V6/update
      ```

      ii. Extract the 6.0.1-WP-Multi-RP001.jar from the zip file and transfer the resulting files and folders to the newly created /QIBM/ProdData/PortalExpress/V6/update folder.

   c. For the 6.0.1-WP-Multi-RP001.zip file:

      i. Create a folder called `fixpacks` in the /QIBM/ProdData/PortalExpress/V6/update directory:

      ```
      mkdir /QIBM/ProdData/PortalExpress/V6/update/fixpacks
      ```

      ii. Extract the 6.0.1-WP-Multi-RP001.jar from the zip file and transfer it to the newly created folder /QIBM/ProdData/PortalExpress/V6/update/fixpacks.

   d. For the 6.0.1-WP-WSASv6.0.2.17-IFPackage.zip file:

      i. Unzip the 6.0.1-WP-WSASv6.0.2.17-IFPackage.zip file and any contained zip files to obtain at least the following interim fixes with the *.pak extension. Do *not* attempt to unzip or unpack the *.pak files:

```
PK37272_ifix.pak
6.0.2.17-WS-WAS-IFPK32424.pak
6.0.2.17-WS-WAS-IFPK34800.pak
6.0.2.17-WS-WAS-IFPK40359.pak
6.0.2.17-WS-WAS-IFPORTAL_NPE_PK41358.pak
```

ii. Transfer or ftp the *.pak files to the following folder:

```
/QIBM/ProdData/WebSphere/AppServer/V6/Base/updateinstaller/maintenance
```

If you are running the Network Deployment option, transfer to the following folder:

```
/QIBM/ProdData/WebSphere/AppServer/V6/ND/updateinstaller/maintenance
```

4. Install the required interim WebSphere Application Server fixes (*.pak files):

   a. Change the directory to the updateinstaller folder. If you are running the Network Deployment option, replace `Base` with `ND`:

   ```
   cd /QIBM/ProdData/WebSphere/AppServer/V6/Base/updateinstaller
   ```

   b. Run the update command in the maintenance folder to apply all the interim fixes. Following are the individual commands. If you are running the Network Deployment option, replace `Base` with `ND` in the following commands:

   ```
   update -W maintenance.package="/QIBM/ProdData/WebSphere/AppServer/V6/Base/u
   pdateinstaller/maintenance/PK37272_ifix.pak"

   update -W maintenance.package="/QIBM/ProdData/WebSphere/AppServer/V6/Base/u
   pdateinstaller/maintenance/6.0.2.17-WS-WAS-IFPK32424.pak"

   update -W maintenance.package="/QIBM/ProdData/WebSphere/AppServer/V6/Base/u
   pdateinstaller/maintenance/6.0.2.17-WS-WAS-IFPK34800.pak"

   update -W maintenance.package="/QIBM/ProdData/WebSphere/AppServer/V6/Base/u
   pdateinstaller/maintenance/6.0.2.17-WS-WAS-IFPK40359.pak"

   update -W maintenance.package="/QIBM/ProdData/WebSphere/AppServer/V6/Base/u
   pdateinstaller/maintenance/6.0.2.17-WS-WAS-IFPORTAL_NPE_PK41358.pak"
   ```

5. The installation process removes the plain text passwords from various properties files in /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/PortalServer/config folder, including:

   – wpconfig.properties
   – wpconfig_dbdomain.properties
   – wpconfig_sourceDb.properties

   If you want to keep these passwords, add the following line to the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/portalexpress/PortalServer/config wpconfig.properties file:

   ```
   PWordDelete=false
   ```

6. WebSphere Portal Server search collections are not compatible between versions. This might be an issue in an environment with multiple versions. See *Migrating your search collections between portal versions* in the WebSphere Portal Information Center available at the following Web site to ensure the existing collections are preserved and not replaced by the installation process. You might need to export the current collection and later import it to the new version after the upgrade.

   http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp?topic=/com.ibm.wp.ent.doc/wps/srtmigratcoll.html

7. Change the timeout request for the Simple Object Access Protocol (SOAP) client, the default value is 180 seconds:
   a. From the i5/OS command line, edit the soap.client.props file in the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/properties folder. For example, for a portal profile called portalexpress:

      ```
      EDTF
      STMF('/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/portalexpress/properties/s
      oap.client.props')
      ```

   b. Change the timeout request line and set as follows:

      ```
      com.ibm.SOAP.requestTimeout=6000
      ```

   c. Save the changes.
8. Using the WebSphere Administrative Console, change the HTTP connection timeout value for the various HTTP transport chains for the WebSphere_Portal server Web container.
   a. Log on to the WebSphere Administrative Console.
   b. Click **Servers** → **Application Servers**.
   c. Click **WebSphere_Portal**.
   d. Click **Web Container settings** → **Web container transport chains**.
   e. For each of the transport chains listed (usually there are four):
      i. Click **HTTP Inbound Channel.**
      ii. Change the value of Read timeout to **180**.
      iii. Change the value of Write timeout to **180**.
      iv. Click **Apply** and then click **OK**.
   f. Save all your changes.
9. From the i5/OS command line, edit the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/PortalServer/config/wpconfig.properties file and fill in the appropriate values for the following parameters:
   – PortalAdminPwd
   – WasPassword
10. From the i5/OS command line, edit the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/PortalServer/config/wpconfig_dbdomain.properties file and fill in the appropriate values for the following parameters:
    – release.DbPassword
    – customization.DbPassword
    – community.DbPassword
    – jcr.DbPassword
    – wmm.DbPassword
    – feedback.DbPassword
    – likeminds.DbPassword
    – designer.DbPassword

    Tip: The passwords for the databases are all the same and usually set to the same value as the WebSphere Portal administrator password.

11. Assign a password to the QEJBSVR user profile. By default, QEJBSVR is shipped with a password of *NONE. The process to apply fix pack 6.0.1 requires the QEJBSVR user

profile to have a password. From a 5250 Command Entry session, enter the command: `CHGUSRPRF USRPRF(QEJBSVR) PASSWORD(<password>)`.

Note: Change the QEJBSVR password back to *NONE after applying the portal fix pack.

Upgrading to WebSphere Portal Express V6.0.1

Important: Complete the necessary preparation steps in the previous section before proceeding with the upgrading steps in this section.

To upgrade to WebSphere Portal Express V6.0.1, perform the following steps:

1. From the QShell (`STRQSH`) environment, run the following command to set up the Java environment for the installation process:
   - For Base:

     ```
     export WAS_PROD_HOME=/QIBM/ProdData/WebSphere/AppServer/V6/Base
     ```

   - For Network Deployment (ND):

     ```
     export WAS_PROD_HOME=/QIBM/ProdData/WebSphere/AppServer/V6/ND
     ```

2. Stop all the servers. If you are running the Network Deployment option, replace `Base` with `ND` in the following commands:

   ```
   cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/bin

   stopServer server1 -profileName <profile_root> -user was_admin_userid -password
   was_admin_password

   stopServer WebSphere_Portal -profileName <profile_name> -user was_admin
   -password was_admin_pwd
   ```

3. Install the fix pack. If you are running the Network Deployment option, replace `Base` with `ND` in the following commands:

   ```
   cd /QIBM/ProdData/PortalExpress/V6/update

   updatePortal.sh  -install -installDir
   "/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/PortalServer
   " -fixpack -fixpackDir "/QIBM/ProdData/PortalExpress/V6/update/fixpacks"
   -fixpackID WP_PTF_601
   ```

   For example, for a portal profile called Express60, use the following command:

   ```
   updatePortal.sh  -install -installDir
   "/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/Express60/PortalServer"
   -fixpack -fixpackDir "/QIBM/ProdData/PortalExpress/V6/update/fixpacks"
   -fixpackID WP_PTF_601
   ```

4. The installation runs for a few hours. The output is generated in the configtrace.log file of the portal profile being upgraded. In our example, the output is found in the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/Express60/PortalServer/log/configtrace.log file.

Tip: If the installation ends due to errors, correct the errors and rerun the command again. Before you restart the installation:

- Remove the /QIBM/ProdData/WebSphere/AppServer/V6/Base/deploytool/itp/configuration directory and try it again to see if it fixes the problem. This directory will be regenerated.
- Make sure the user running the installation has write access to the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/PortalServer/ log folder and the configtrace.log file (if it exists).
- Delete, remove, or rename the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/PortalServer/config/AppsTargets.log file.

At this point, you have successfully run the main upgrade commands. However, you must complete the post-installation steps before you can use the portal server.

Post-installation steps

Important: You must run the post-installation steps in this section. Otherwise, you cannot log in to the WebSphere Portal Express server.

The installation process does not automatically update the screens in the wps.ear application even if it updates everything like the theme, skins, JSPs, and so on. To have the screens updated automatically, update the wpconfig.properties with the following entry as part of the pre-upgrade steps discussed in “Preparing for the upgrade” on page 348.

```
CopyWpsEarScreens=true
```

If you set the `CopyWpsEarScreens=true` parameter, ignore the first seven steps of the following post-installation steps and go to Step 8 on page 354.

If you did not set the `CopyWpsEarScreens=true` parameter, and you still want to process the new windows, proceed with the following steps.

Following is a list of screen files that have been modified in WebSphere Portal Express V6.0.1. The files have been placed in the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/PortalServer/fixes directory during the upgrade process and you are required to manually merge the updated files into the wps.ear file:

```
/screens/chtml/Error.jsp
/screens/chtml/ErrorLoginRetrieveUser.jsp
/screens/chtml/ErrorNotAuthorized.jsp
/screens/chtml/ErrorNotLoggedIn.jsp
/screens/chtml/Help.jsp
/screens/chtml/Home.jsp
/screens/chtml/Login.jsp
/screens/chtml/SelectPage.jsp
/screens/html/BidiInclude.jsp
/screens/html/Congrats.jsp
/screens/html/Error.jsp
/screens/html/ErrorLoginRetrieveUser.jsp
```

```
/screens/html/ErrorNotAuthorized.jsp
/screens/html/ErrorNotLoggedIn.jsp
/screens/html/ErrorSessionTimeout.jsp
/screens/html/ForgotPassword.jsp
/screens/html/Home.jsp
/screens/html/Login.jsp
/screens/html/RegistrationError.jsp
/screens/html/UserProfileConf.jsp
/screens/html/UserProfileForm.jsp
/screens/wml/Error.jsp
/screens/wml/ErrorLoginRetrieveUser.jsp
/screens/wml/ErrorNotAuthorized.jsp
/screens/wml/ErrorNotLoggedIn.jsp
/screens/wml/Home.jsp
/screens/wml/Login.jsp
/screens/wml/SelectPage.jsp
```

The basic steps for merging these new screens with the existing ones in the wps.ear application are described in *Deploying customized themes and skins* in the WebSphere Portal Information Center at:

http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp?topic=/com.ibm.wp.ent.doc/wps/dgn_dpycst.html

The caveat here is that you replace or add screen files instead of the usual themes and skins files. The following steps are an example of this process:

1. Start the server1 process associated with the portal profile. If you are running the Network Deployment option, replace `Base` with `ND` in the following commands:

   ```
   cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/bin

   startServer server1 -profileName <profile_root> -user was_admin_userid
   -password was_admin_password
   ```

2. Export the WebSphere Portal EAR file, wps.ear, as follows in the QShell (`STRQSH`) environment:

   a. Change directory to the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/bin folder:

      ```
      cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/bin
      ```

   b. Invoke the wsadmin utility to extract and export the wps.ear application to a temporary directory. The directory already exists.

      ```
      wsadmin -profileName <profile_root> -user admin_user_id -password admin_password -c
      '$AdminApp export wps  <directory>/wps.ear'
      ```

3. Use the EARExpander tool to expand the contents of the exported EAR file:

   a. Create a directory called wps_expanded, preferably in the same folder where the wps.ear file was exported:

      ```
      mkdir <directory>/wps_expanded
      ```

   b. Run the EARExpander to expand the application in the newly created folder:

      ```
      EARExpander -ear directory/wps.ear -operationDir <directory>/wps_expanded -operation
      expand
      ```

4. Compare, add to, or replace the windows in the <*directory*>/wps_expanded/wps.war/screens/html/ folder with the new ones that exist in the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/PortalServer/fixes/wps.ear/wps.ear/wps.war/screens/html folder.
5. Rename the current exported wps.ear file:

   ```
   mv <directory>/wps.ear <directory>/wpsold.ear
   ```

6. Use the EARExpander command to collapse the EAR directory back into a new and updated wps.ear file:

   ```
   EARExpander -ear <directory>/wps.ear -operationDir <directory>/wps_expanded
   -operation collapse
   ```

7. Use the wsadmin command to update the wps.ear file:

   ```
   wsadmin -profileName <profilename> -user admin_user_id -password admin_password
   -c '$AdminApp install <directory>/wps.ear {-update -appname wps -nodeployejb}'
   ```

8. The installation process automatically deletes passwords during the install.The passwords are preserved if you set `PWordDelete=false` in the wpconfig.properties. You can manually delete passwords after running the upgrade using the following steps:
   a. Add the following parameter to the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/config/wpconfig.properties file:

      ```
      PWordDelete=true
      ```

   b. Run the following command to delete the password:

      ```
      cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/config
      WPSconfig.sh -profileName <profilename> action-delete-passwords-601
      ```

9. Using the WebSphere Administrative Console, remap WebSphere Portal to the external Web server:
   a. Start server1 associated with the profile, if it is not started. It might have started as part of the previous steps. If necessary, use the following QShell (STRQSH) commands to start it:

      ```
      cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/bin

      startServer server1 -profileName <profile_root> -user was_admin_userid
      -password was_admin_password
      ```

   b. Log on to the WebSphere Administrative Console.
   c. Click **Applications** → **Enterprise Applications**.
   d. Navigate to and click **wps**.
   e. Click **Map modules to servers**.
   f. Select all four of the modules shown by checking all four boxes next to the modules.
   g. From the Clusters and Servers drop-down menu, select both the Web server and WebSphere Portal. You might need to hold down the CTRL key to select both. Click **Apply** next to the Clusters and Servers window.
   h. Click **Apply** at the bottom of the screen and save all changes.

10. Using the WebSphere Administrative Console, regenerate the Apache HTTP server plugin:
    a. Start server1 associated with the profile, if it is not started. It might have started as part of the previous steps. If necessary, use the following QShell (STRQSH) commands to start it:

    ```
    cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/bin

    startServer server1 -profileName <profile_root> -user was_admin_userid
    -password was_admin_password
    ```

    b. Log on to the WebSphere Administrative Console.
    c. Click **Servers** → **Web servers**.
    d. Select the plugin and click **Generate Plugin**.
    e. Click **Propagate Plugin.** If you are using a remote Web server, you might need to copy the plugin to the remote Web server.
11. Restart the IBM WebSphere Portal Express V6.0 server. Also restart the associated HTTP server:

    ```
    cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profilename>/bin

    startServer WebSphere_Portal -profileName <profile_name> -user was_admin -password
    was_admin_pwd
    ```

12. If you are running IBM Workplace Web Content Management™, perform the following steps:
    a. Redeploy your customizations, including customized JSPs to the Web Content Management enterprise application and the customized local rendering portlet using the same process you used initially to deploy them.
    b. Refresh all existing items by opening and saving each item. To do this, you must run the RefreshAllItems task by entering the following URL in a Web browser, replacing the *hostname* with the one appropriate for your environment. This option updates the last saved date to the current date and time.

    ```
    http://hostname.yourco.com:port_number/wps/wcm/connect?MOD=RefreshAllItems&l
    ibraryname
    ```

    If you want to preserve the last saved date of each item, use the following URL instead, again replacing the *hostname* with the appropriate values for your environment:

    ```
    http://hostname.yourco.com:port_number/wps/wcm/connect?MOD=RefreshAllItems&l
    ibrary=libraryname&preserve_dates=true
    ```

Important: The Web content storage format used in WebSphere Portal V6.0 was updated in the V6.0.1 cumulative fix. Any data created in V6.0.1, or upgraded from V6.0 using the RefreshAllItems task is not compatible with WebSphere Portal V6.0. If you uninstall the V6.0.1 cumulative fix, you need to install the V6.0.0.1 cumulative fix for WebSphere Portal.

We recommend that you back up your V6.0 database prior to running the RefreshAllItem" task. This restores any Web content created prior to installing the V6.0.1 cumulative fix to a 6.0 version of WebSphere Portal.

13. Confirm that WebSphere Portal Express has been successfully upgraded to version 6.0.1:

    a. You also need to restart the IBM Web Administration for i5/OS server for the new version to show up:

    ```
    ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

    STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
    ```

    b. Review the contents of /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/PortalServer /log/VersionInfo.log. For example:

    ```
    IBM WebSphere Portal 6.0.1
    Build Level: wp601_194 (2007-04-01 10:52)
    Server Name: WebSphere_Portal
    Started at:  4/12/2007 11:28:03:185 EDT

    Installed FixPacks:
        WP_PTF_601 (IBM WebSphere Portal, Version 6.0.1.0 Fix Pack)
    Installed Interim Fixes:
        None
    ```

    c. After the WebSphere Portal server has been restarted, review the contents of /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/Po rtalServer/log/systemOut.log. For example:

    ```
    [4/9/07 23:02:43:319 EDT] 00000013 LogManagerDef I
    com.ibm.wps.logging.LogManagerDefaultImpl init
    ------------------------------------------------------------------------------
    IBM WebSphere Portal 6.0.1
    Licensed Materials - Property of IBM
    5724-E76 and 5655-R17
    (C) Copyright IBM Corp. 2001, 2006 - All Rights Reserved.
    US Government Users Restricted Rights - Use, duplication or disclosure restricted by
    GSA ADP Schedule Contract with IBM Corp.
    ------------------------------------------------------------------------------
    Build Level:
    wp601_194 (2007-04-01 10:52)
    ------------------------------------------------------------------------------
    [4/9/07 23:02:44:485 EDT] 00000013 ProductServic I
    com.ibm.wps.services.product.ProductServiceImpl findInstalledFixes EJPFD0051I: The
    following fix packs have been installed:
        WP_PTF_601 (IBM WebSphere Portal, Version 6.0.1.0 Fix Pack)
    [4/9/07 23:02:44:551 EDT] 00000013 ProductServic I
    com.ibm.wps.services.product.ProductServiceImpl findInstalledFixes EJPFD0054I: No
    interim fixes have been installed.
    ```

    d. Review the output of the /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<*profilename*>/PortalServer /bin/WPVersionInfo.sh command. This gives the most comprehensive report:

    ```
    cd
    /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/
    bin

    WPVersionInfo.sh

    WVER0010I: Copyright (c) IBM Corporation 2002, 2006; All rights reserved.
    WVER0011I: WebSphere Portal
    WVER0012I: VersionInfo reporter version 1.10.1.1, dated 7/29/05

    excluding product file name is itlm.product
    ```

```
--------------------------------------------------------------------------------
IBM WebSphere Portal Product Installation Status Report
--------------------------------------------------------------------------------

Report at date and time 2007-05-01T12:50:30-05:00

Installation
--------------------------------------------------------------------------------
Product Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer
Version Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/
version
DTD Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/
version/dtd
Log Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/
version/log
Backup Directory
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/WP6XSERVER/PortalServer/
version/backup
TMP Directory       /tmp

Installation Platform
--------------------------------------------------------------------------------
Name           IBM WebSphere Portal
Version        6.0

Technology List
--------------------------------------------------------------------------------
MP             installed
PDM            installed
WCM            installed
PZN            installed

Installed Product
--------------------------------------------------------------------------------
Name           IBM WebSphere Portal MultiPlatform
Version        6.0.1.0
ID             MP
Build Level    wp601_194_01
Build Date     04/01/2007

Installed Product
--------------------------------------------------------------------------------
Name           IBM WebSphere Portal Document Manager
Version        6.0.1.0
ID             PDM
Build Level    wp601_194_01
Build Date     04/01/2007

Installed Product
--------------------------------------------------------------------------------
Name           IBM WebSphere Portal Personalization
```

```
Version        6.0.1.0
ID             PZN
Build Level    wp601_194_01
Build Date     04/01/2007

Installed Product
--------------------------------------------------------------------------------
Name           IBM WebSphere WebSphere Portal Web Content Manager
Version        6.0.1.0
ID             WCM
Build Level    wp601_194_01
Build Date     04/01/2007
--------------------------------------------------------------------------------
End Installation Status Report
--------------------------------------------------------------------------------
```

B

Additional material

This Redpaper refers to additional material that you can download from the Internet.

Locating the Web material

The Web material associated with this Redpaper is available in softcopy on the Internet from the IBM Redbooks publications Web server. Point your Web browser at:

`ftp://www.redbooks.ibm.com/redbooks/REDP4303`

Alternatively, you can go to the IBM Redbooks Web site at:

`ibm.com/redbooks`

Select **Additional materials** and open the directory that corresponds with the IBM Redpaper form number, REDP4303.

Using the Web material

The additional Web material that accompanies this Redpaper includes the following files:

- ExpressSave.sh: This script collects the private authorities of all objects (for QTMHHTTP and QEJBSRV) before they are saved. It also runs the Save Security Data (SAVSECDTA) CL command to collect the portal profile's database administrator's user profile to a save file. The output files are saved with the backup and subsequently deleted.
- PreExpressRestore.sh: This script is only used as a cleanup script prior to a restore where you want to restore all libraries and integrated file system objects.
- PostExpressRestore.sh: This script restores the private authorities of all the integrated file system objects (for QTMHHTTP and QEJBSRV) that were collected when the backup was run. It also restores the user profile that owns the databases associated with the portal profile being restored. The private authority of the user profile is also restored.

© Copyright IBM Corp. 2007. All rights reserved.

Refer to 6.3, “Online backup using BRMS” on page 245 for information about how to use these scripts.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks publications

For information about ordering these publications, see “How to get IBM Redbooks publications” on page 362. Note that some of the documents referenced here may be available in softcopy only:

- *Enabling Collaboration in WebSphere Portal Express V6 on i5/OS*, REDP-4310
- *Implementation and Practical Use of LDAP on the IBM eServer iSeries Server*, SG24-6193
- *Portal Express Version 6 - Customizing Portal Express for Small to Medium Business*, REDP-4316
- *Implementing IBM Lotus Domino 7 for i5/OS*, SG24-7311
- *Improve Whole System Backups with the New Save-While-Active Function*, REDP-7200

Other publications

These publications are also relevant as further information sources:

- *Backup Recovery and Media Services for iSeries, Version 5*:

  http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc415345.pdf
- *Backup Recovery and Media Services for iSeries, BRMS iSeries Navigator Client Student Guide:*

  http://www.ibm.com/servers/eserver/iseries/service/brms/pdf/StudentGuide54.pdf

Online resources

These Web sites are also relevant as further information sources:

- WebSphere Portal Version 6 Information Center:

  http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp
- WebSphere Application Server for i5/OS Information Center:

  http://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/index.jsp
- WebSphere Portal Express V6.0 downloadable files:

  http://www.ibm.com/support/docview.wss?rs=688&uid=swg24014177
- Workload Estimator:

  http://www-912.ibm.com/wle/EstimatorServlet
- Fix Central:

© Copyright IBM Corp. 2007. All rights reserved.

http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp

- System i Group PTFs:

  http://www-912.ibm.com/s_dir/slineO03.NSF/GroupPTFs?OpenView&view=GroupPTFs

- Support for IBM System i:

  http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/brandmain?brandind=5000027

- Preventive Service Planning:

  http://www-912.ibm.com/s_dir/slineO03.NSF/GroupPTFs

How to get IBM Redbooks publications

You can search for, view, or download IBM Redbooks publications, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy IBM Redbooks publications, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Installing and Configuring WebSphere Portal Express V6 on i5/OS

Redpaper

Comprehensive step-by-step guide

Tips and common pitfalls explained

Practical performance tuning guidelines

This IBM Redpaper provides an overview of the WebSphere Portal V6.0 family on the System i platform and positions WebSphere Portal Express V6.0 within the portal family. This Redpaper provides information about how to prepare your System i i5/OS environment before you install and configure WebSphere Portal Express V6. It includes step-by-step instructions that help system administrators and IT consultants to quickly deploy WebSphere Portal Express into a production environment on a System i machine.

This Redpaper also incudes information that helps you perform the initial tuning of your portal environment. It explains how to configure Secure Sockets Layer (SSL) to protect sensitive login information to the portal and LDAP servers. Finally, it explains how to save a WebSphere Portal Express V6 profile while it is online and actively in use.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

REDP-4303-00